

PATENT COOPERATION TREATY

PCT

NOTIFICATION OF THE RECORDING
OF A CHANGE(PCT Rule 92bis.1 and
Administrative Instructions, Section 422)

From the INTERNATIONAL BUREAU

To:

OVD KINEGRAM AG
Gubelstrasse 22
CH-6301 Zug
SUISSE

Date of mailing (day/month/year) 31 July 2000 (31.07.00)	IMPORTANT NOTIFICATION
Applicant's or agent's file reference P2900WO	
International application No. PCT/EP99/10141	International filing date (day/month/year) 20 December 1999 (20.12.99)

1. The following indications appeared on record concerning:		
<input type="checkbox"/> the applicant	<input type="checkbox"/> the inventor	<input checked="" type="checkbox"/> the agent
<input type="checkbox"/> the common representative		
Name and Address SIEMENS BUILDING TECHNOLOGIES AG Corporate Intellectual Property Rights Gubelstrasse 22 CH-6300 Zug Switzerland	State of Nationality	State of Residence
	Telephone No.	
	Facsimile No.	
	Teleprinter No.	
2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:		
<input type="checkbox"/> the person	<input type="checkbox"/> the name	<input type="checkbox"/> the address
<input type="checkbox"/> the nationality	<input type="checkbox"/> the residence	
Name and Address	State of Nationality	State of Residence
	Telephone No.	
	Facsimile No.	
	Teleprinter No.	
3. Further observations, if necessary: The agent has renounced his appointment. Correspondence should now be addressed to the applicant, as indicated in the addressee box above.		
4. A copy of this notification has been sent to:		
<input checked="" type="checkbox"/> the receiving Office	<input checked="" type="checkbox"/> the designated Offices concerned	
<input type="checkbox"/> the International Searching Authority	<input type="checkbox"/> the elected Offices concerned	
<input type="checkbox"/> the International Preliminary Examining Authority	<input checked="" type="checkbox"/> other: Former agent	

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer Aino Metcalfe
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

VERTRAG ÜBER INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

REC'D 26 FEB 2001

WIPO

PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

T 16



Aktenzeichen des Anmelders oder Anwalts T 2900WO/hs	WEITERES VORGEHEN siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsberichts (Formblatt PCT/IPEA/416)	
Internationales Aktenzeichen PCT/EP99/10141	Internationales Anmeldedatum (Tag/Monat/Jahr) 20/12/1999	Prioritätsdatum (Tag/Monat/Tag) 24/12/1998
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK B42D15/10		
Anmelder OVD KINEGRAM AG et al		

- Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationalen vorläufigen Prüfung beauftragten Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.
- Dieser BERICHT umfaßt insgesamt 6 Blätter einschließlich dieses Deckblatts.
 - ☒ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

Diese Anlagen umfassen insgesamt 3 Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

- I ☒ Grundlage des Berichts
- II ☐ Priorität
- III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
- IV ☐ Mangelnde Einheitlichkeit der Erfindung
- V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
- VI ☐ Bestimmte angeführte Unterlagen
- VII ☐ Bestimmte Mängel der internationalen Anmeldung
- VIII ☒ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags 10/07/2000	Datum der Fertigstellung dieses Berichts 22.02.2001
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde:  Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Bevollmächtigter Bediensteter Schreiber, M Tel. Nr. +49 89 2399 2831 

I. Grundlage des Berichts

1. Dieser Bericht wurde erstellt auf der Grundlage (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigelegt, weil sie keine Änderungen enthalten.*):

Beschreibung, Seiten:

1-10 ursprüngliche Fassung

Patentansprüche, Nr.:

1-18 eingegangen am 20/12/2000 mit Schreiben vom 18/12/2000

Zeichnungen, Blätter:

1/3-3/3 ursprüngliche Fassung

2. Hinsichtlich der **Sprache**: Alle vorstehend genannten Bestandteile standen der Behörde in der Sprache, in der die internationale Anmeldung eingereicht worden ist, zur Verfügung oder wurden in dieser eingereicht, sofern unter diesem Punkt nichts anderes angegeben ist.

Die Bestandteile standen der Behörde in der Sprache: zur Verfügung bzw. wurden in dieser Sprache eingereicht; dabei handelt es sich um

- ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen Recherche eingereicht worden ist (nach Regel 23.1(b)).
- ☐ die Veröffentlichungssprache der internationalen Anmeldung (nach Regel 48.3(b)).
- ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen vorläufigen Prüfung eingereicht worden ist (nach Regel 55.2 und/oder 55.3).

3. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale vorläufige Prüfung auf der Grundlage des Sequenzprotokolls durchgeführt worden, das:

- ☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.
- ☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.
- ☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.
- ☐ Die Erklärung, daß die in computerlesbarer Form erfassten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

4. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/EP99/10141

- ☐ Beschreibung, Seiten:
☐ Ansprüche, Nr.:
☐ Zeichnungen, Blatt:

5. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)).

(Auf Ersatzblätter, die solche Änderungen enthalten, ist unter Punkt 1 hinzuweisen; sie sind diesem Bericht beizufügen).

6. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja: Ansprüche	2,5-18
	Nein: Ansprüche	1,3,4
Erfinderische Tätigkeit (ET)	Ja: Ansprüche	9-18
	Nein: Ansprüche	1-8
Gewerbliche Anwendbarkeit (GA)	Ja: Ansprüche	1-18
	Nein: Ansprüche	

2. Unterlagen und Erklärungen
siehe Beiblatt

VIII. Bestimmte Bemerkungen zur internationalen Anmeldung

Zur Klarheit der Patentansprüche, der Beschreibung und der Zeichnungen oder zu der Frage, ob die Ansprüche in vollem Umfang durch die Beschreibung gestützt werden, ist folgendes zu bemerken:
siehe Beiblatt

Zu Punkt V

Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

Dokument US-A-3 833 795 (= Dokument D1), das als nächstliegender Stand der Technik angesehen wird, offenbart (vgl. die Zusammenfassung, Spalte 2, Zeile 17 - Spalte 4, Zeile 35) ein Dokument (10) mit zwei jeweils sechststelligen Zahlen nebeneinander. Es ist natürlich auch möglich diese zwei sechststelligen Zahlen als drei jeweils vierstellige Zahlen zu lesen, wobei man der ersten den Namen "Kennung", der zweiten den Namen "Dokumentennummer" und der dritten den Namen "Kontrollnummer" geben kann. Damit hat das Dokument gemäß Dokument D1 eine wenigstens maschinell lesbare Dokumentennummer auf dem Substrat und ein Speicherfeld (der Ort, wo die dritte Nummer gedruckt ist) für die Aufnahme der Kontrollnummer, die maschinell lesbar ist, wobei auf dem Substrat eine optische Markierung mit der maschinell lesbaren Kennung angebracht ist.

Der Gegenstand des Anspruchs 1 unterscheidet sich von diesem Stand der Technik nicht (siehe auch Punkt VIII).

Der Gegenstand des Anspruchs 1 ist somit nicht neu (Artikel 33 (2) PCT).

Die abhängigen Ansprüche 2 - 8 enthalten keine Merkmale, die in Kombination mit den Merkmalen irgendeines Anspruchs, auf den sie sich beziehen, die Erfordernisse des PCT in Bezug auf Neuheit bzw. erfinderische Tätigkeit erfüllen. Die Gründe dafür sind die folgenden:

Bei dem zusätzlichen Merkmal des Anspruchs 2 handelt es sich nur um eine von mehreren naheliegenden Möglichkeiten, aus denen der Fachmann ohne erfinderisches Zutun den Umständen entsprechend auswählen würde.

Ein Scheck gemäß Dokument D1 weist zwangsläufig auch die zusätzlichen Merkmale der Ansprüche 3 und 4 auf.

Bei den zusätzlichen Merkmalen der Ansprüche 5 - 8 handelt es sich nur um eine von mehreren naheliegenden Möglichkeiten, aus denen der Fachmann ohne erfinderisches Zutun den Umständen entsprechend auswählen würde, um Daten in einem

Wertdokument zu speichern.

Das Dokument D1, das als nächstliegender Stand der Technik angesehen wird, offenbart (vgl. die Zusammenfassung, Spalte 2, Zeile 17 - Spalte 4, Zeile 35) ein System von dem sich der Gegenstand des Anspruchs 9 mindestens dadurch unterscheidet, dass das System ein Validiergerät beinhaltet, wobei im Validiergerät eine Recheneinheit für kryptographische Operationen mit einem ersten geheimen Schlüssel zum Erzeugen einer Kontrollnummer durch Verschlüsseln von wenigstens zwei Parametern, der Dokumentennummer und der Kennung, vorhanden ist und dass ein Aufzeichnungsmittel zum Einschreiben der Kontrollnummer in das wenigstens maschinell lesbare Speicherfeld eingerichtet ist,

Der Gegenstand des Anspruchs 9 ist somit neu (Artikel 33 (2) PCT).

Die mit der vorliegenden Erfindung zu lösende Aufgabe kann somit darin gesehen werden, die Möglichkeit zu schaffen, ein in großen Mengen kostengünstig hergestelltes Dokument derart zu sichern, dass seine Echtheitsmerkmale erst beim Inverkehrbringen vervollständigt werden, so dass ein Diebstahl in dem Zeitraum von der Herstellung bis zur Übergabe des Dokuments an die berechnigte Person kein Problem mehr darstellt. Die in Anspruch 9 der vorliegenden Anmeldung für diese Aufgabe vorgeschlagene Lösung beruht aus den folgenden Gründen auf einer erfinderischen Tätigkeit (Artikel 33(3) PCT):

In dem vorliegenden Stand der Technik ist kein Hinweis auf die unterscheidenden Merkmale zu finden.

Die Ansprüche 10 - 18 sind vom Anspruch 9 abhängig und erfüllen damit ebenfalls die Erfordernisse des PCT in bezug auf Neuheit und erfinderische Tätigkeit.

Zu Punkt VIII

Bestimmte Bemerkungen zur internationalen Anmeldung

Anspruch 9 ist aus folgendem Grund nicht klar:

Laut Anspruch 1 ist das Dokument durch Einschreiben der Kontrollnummer in das Speicherfeld bereits vervollständigt. Daher werden die Merkmale des Anspruchs 9 bezüglich des Validiergeräts sinnlos (das Dokument ist ja bereits validiert). Das System

gemäß Anspruch 9 hätte daher eher ein Dokument ohne Kontrollnummer enthalten sollen.

Das Merkmal in dem Vorrichtungsanspruch 1, dass die Kontrollnummer erst bei der Inverkehrbringung im Speicherfeld eingesetzt ist bezieht sich auf ein Verfahren zur Verwendung der Vorrichtung und nicht auf die Definition der Vorrichtung anhand ihrer technischen Merkmale. Die beabsichtigten Einschränkungen gehen daher im Widerspruch zu den Erfordernissen des Artikels 6 PCT nicht klar aus dem Anspruch hervor. Das obige Merkmal wird daher für die Beurteilung der Neuheit und erfinderischen Tätigkeit (siehe obigen Punkt V) nicht in Betracht gezogen.

Außerdem kann das Merkmal, dass die Kontrollnummer das Ergebnis einer kryptographischen Operation mit wenigstens zwei Parametern, der Dokumentennummer und der Kennung, und einem ersten geheimen Schlüssel ist, nicht den Gegenstand des Anspruchs 1 kennzeichnen, da es einer Nummer auf einem einzelnen Dokument (wie beansprucht) nicht anzusehen ist, ob sie aus einer solchen kryptographischen Operation hervorgegangen ist, oder nicht, da jede beliebige Nummer durch irgendeinen kryptographischen Schlüssel erzeugbar ist. Ähnliche Überlegungen gelten für die "Kennung" und die "Dokumentennummer", weil ja nur ein einzelnes Dokument beansprucht wird. Jedes dieser Merkmale bedeutet also nichts weiter als "Nummer" (siehe obigen Punkt V).

Die Formulierung "dass zur Aktivierung ein Echheitszertifikat die wenigstens maschinell lesbare Information im Speicherfeld durch Einschreiben der ... Kontrollnummer in das Speicherfeld erst bei der Inverkehrbringung vervollständigt ist" ist grammatikalisch nicht korrekt. Außerdem bleibt unklar, was das Echtheitszertifikat ist und in welchem Zusammenhang es zum beanspruchten Dokument steht.

PATENTANSPRÜCHE

1. Dokument (1) mit einer wenigstens maschinell lesbaren Dokumentennummer (2) auf dem Substrat (6) und einem Speicherfeld (4) für die Aufnahme einer wenigstens maschinell lesbaren Kontrollnummer (9), dadurch gekennzeichnet, dass auf dem Substrat (6) eine optische Markierung (3) mit einer maschinell lesbaren Kennung (7) angebracht ist, und dass zur Aktivierung ein Echtheitszertifikat (23) die wenigstens maschinell lesbare Information im Speicherfeld (4) durch Einschreiben der das Ergebnis einer kryptographischen Operation mit wenigstens zwei Parametern, der Dokumentennummer (2) und der Kennung (7), und einem ersten geheimen Schlüssel (10) bildenden Kontrollnummer (9) in das Speicherfeld (4) erst bei der Inverkehrbringung vervollständigt ist.
2. Dokument (1) nach Anspruch 1, dadurch gekennzeichnet, dass die optische Markierung (3) beugungsoptische Strukturen aufweist, und dass wenigstens ein Teil der beugungsoptischen Strukturen die maschinell lesbare Kennung (7) enthält.
3. Dokument (1) nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass das Substrat (6) ein Kontrollfeld (5) für die Aufnahme eines wenigstens visuell lesbaren, individuellen und auf eine Person bezogenen Codes (11) aufweist.
4. Dokument nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass das Speicherfeld (4) auf dem Substrat (6) angeordnet ist und dass nach der Aktivierung die Kontrollnummer (9) im Speicherfeld (4) in wenigstens maschinell lesbaren Zeichen enthalten ist.
5. Dokument (1) nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass im Substrat (6) ein Mikrochip (13) eingelassen ist, dass das Speicherfeld (4) im Speicher (14) des Mikrochips (13) angeordnet ist und dass nach der Aktivierung das Speicherfeld (4) die Kontrollnummer (9) enthält und der einmal eingeschriebene Inhalt des Speicherfelds (4) elektronisch nicht veränderbar ist.
6. Dokument (1) nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass auf dem Substrat (6) ein Magnetstreifen (16) mit dem Speicherfeld (4) angeordnet ist, dass der Magnetstreifen (16) wenigstens das Speicherfeld (4) enthält und dass nach der Aktivierung das Speicherfeld (4) die magnetisch lesbare Kontrollnummer (9) aufweist.
7. Dokument (1) nach Anspruch 1, 2, 3 oder 4, dadurch gekennzeichnet, dass auf dem Substrat (6) ein optischer Informationsträger (17, 17') angeordnet ist, dass der optische Informationsträger (17, 17') wenigstens das Speicherfeld (4) enthält und dass nach der Aktivierung der nicht mehr veränderbare optische Informationsträger (17, 17'') im Speicherfeld (4) die Kontrollnummer (9) in optisch lesbaren Zeichen aufweist.
8. Dokument (1) nach Anspruch 7, dadurch gekennzeichnet, dass ein Teil des optischen Informationsträgers (17, 17') die optische Markierung (3) bildet und die Kennung (7) enthält.

9. System (20) bestehend aus wenigstens einem Dokument (1) nach einem der Ansprüche 1 bis 8, einem Validiergerät (21) und einem Verifikator (22),
dadurch gekennzeichnet,
dass im Validiergerät (21) eine Transportvorrichtung (25) zur Aufnahme des Dokuments (1), ein
5 Aufzeichnungsmittel (27) und ein optischer Leser (26) zum maschinellen Ablesen von wenigstens der Kennung (7) angeordnet sind, dass das Validiergerät (21) weiter eine mit dem Aufzeichnungsmittel (27) und dem optischen Leser (26) verbundene Recheneinheit (24) für kryptographische Operationen mit einem ersten geheimen Schlüssel (10) zum Erzeugen der Kontrollnummer (9) durch Verschlüsseln von wenigstens zwei Parametern, der Dokumentennummer (2) und der vom optischen Leser (26)
10 abgelesene Kennung (7), umfasst, dass das Aufzeichnungsmittel (27) zum Einschreiben der Kontrollnummer (9) zum Aktivieren des Dokuments (1) zum Echtheitszertifikat (23) in das wenigstens maschinell lesbare Speicherfeld (4) eingerichtet ist,
dass der Verifikator (22) wenigstens ein Rechengerät (33), einen optischen Leser (26) zum maschinellen Ablesen der Kennung (7) und ein Aufnahmemittel (32) zum Ausrichten eines zu
15 überprüfenden Echtheitszertifikats (23) zum maschinellen Ablesen aufweist, dass das Rechengerät (33) mit Eingabe- und Ablesemitteln (26; 28; 29) verbunden und für kryptographische Operationen mit einem zweiten Schlüssel (34) sowie zur Überprüfung der Zusammengehörigkeit wenigstens der Kontrollnummer (9) und der zum Verschlüsseln benutzten Parametern der kryptographischen Operation, die auf dem Echtheitszertifikat (23) enthalten sind, und zur Darstellung des
20 Vergleichsergebnisses auf einer Anzeige (31) des Verifikators (22) und/oder zur Erzeugung eines Erlaubnissignals eingerichtet ist.
10. System (20) nach Anspruch 9, dadurch gekennzeichnet, dass der Verifikator (22) eine Tastatur (28) für eine manuelle Eingabe einer persönlichen Identifikationsnummer (PIN) zur Freigabe des Verifikators (22) aufweist und dass der Verifikator (22) zum Überprüfen der persönlichen
25 Identifikationsnummer des Benutzers eingerichtet ist.
11. System (20) nach Anspruch 9 oder 10, dadurch gekennzeichnet, dass der Verifikator (22) eine mit dem Rechengerät (33) verbundene Tastatur (28) für eine manuelle Eingabe der Parameter der kryptographischen Operation an das Rechengerät (33) aufweist, wobei die Parameter wenigstens die Dokumentennummer (2) und die Kontrollnummer (9) umfassen.
- 30 12. System (20) nach einem der Ansprüche 9 oder 11, dadurch gekennzeichnet, dass der Verifikator (22) wenigstens eine mit dem Rechengerät (33) verbundene Leseinheit (29) für eine maschinelle Eingabe der Parameter der kryptographischen Operation an das Rechengerät (33) aufweist, wobei die Parameter wenigstens die Dokumentennummer (2) und die Kontrollnummer (9) umfassen.

13. System (20) nach einem der Ansprüche 9 bis 12, dadurch gekennzeichnet, dass das Validiergerät (21) eine mit der Recheneinheit (24) verbundene Tastatur (28) für eine manuelle Eingabe wenigstens der Dokumentennummer (2) an die Recheneinheit (24) aufweist.
- 5 14. System (20) nach einem der Ansprüche 9 bis 12, dadurch gekennzeichnet, dass das Validiergerät (21) eine mit der Recheneinheit (24) verbundene Leseinheit (29) für eine maschinelle Eingabe der Dokumentennummer (2) an die Recheneinheit (24) aufweist.
- 10 15. System (20) nach einem der Ansprüche 9 bis 14, dadurch gekennzeichnet, dass das Validiergerät (21) für die Eingabe eines individuellen, auf eine berechtigte Person bezogenen Codes (11) mittels einer Tastatur (28) eingerichtet ist, dass das Validiergerät (21) ein Aufzeichnungsmittel (27) im Validiergerät (21) zum Einschreiben des Codes (11) in das Kontrollfeld (5) umfasst und dass der Code (11) einer der Parameter für die Erzeugung der Kontrollnummer (9) im Validiergerät (21) bzw. für die Echtheitsprüfung im Verifikator (22) ist.
- 15 16. System (20) nach einem der Ansprüche 9 bis 15, dadurch gekennzeichnet, dass die Recheneinheit (24) im Validiergerät (21) derart ausgebildet ist, dass bei der Verschlüsselung der Kontrollnummer (9) eine über eine Tastatur (28) eingegebene persönlichen Identifikationsnummer der berechtigten Person als Parameter für die Erzeugung der Kontrollnummer (9) einbezogen ist und dass der Verifikator (22) das Erlaubnissignal nur dann im Rechenggerät (33) erzeugt, wenn bei der Echtheitsprüfung die persönlichen Identifikationsnummer über die Tastatur (28) des Verifikators (22) dem Rechenggerät (33) als Parameter der kryptographischen Operation einbezogen ist.
- 20 17. System (20) nach einem der Ansprüche 9 bis 16, dadurch gekennzeichnet, dass wenigstens ein Validiergerät (21) und wenigstens ein Verifikator (22) über ein Netzwerk (28', 38, 40; 37) mit einem zentralen Rechner (39) zum bidirektionalen Datenaustausch verbunden sind.
- 25 18. System (20) nach einem der Ansprüche 9 bis 17, dadurch gekennzeichnet, dass das wenigstens ein Verifikator (22) über eine Signalleitung (35) mit einer Dienstleistungseinrichtung (36) verbunden ist und dass die Dienstleistungseinrichtung (36) zum Freigeben einer Dienstleistung mittels des über die Signalleitung (35) an die Dienstleistungseinrichtung (36) gesandten Erlaubnissignals eingerichtet ist.

09/868825
Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

10

Applicant's or agent's file reference P2900WO/hs	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/EP99/10141	International filing date (day/month/year) 20 December 1999 (20.12.99)	Priority date (day/month/year) 24 December 1998 (24.12.98)
International Patent Classification (IPC) or national classification and IPC B42D 15/10		RECEIVED NOV 16 2001
Applicant OVD KINEGRAM AG Technology Center 2100		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 6 sheets, including this cover sheet.



This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 3 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☒ Certain observations on the international application

Date of submission of the demand 10 July 2000 (10.07.00)	Date of completion of this report 22 February 2001 (22.02.2001)
Name and mailing address of the IPEA/EP	Authorized officer
Facsimile No.	Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/EP99/10141

I. Basis of the report

1. This report has been drawn on the basis of (Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.):

☐ the international application as originally filed.

☒ the description, pages 1-10, as originally filed,
pages _____, filed with the demand,
pages _____, filed with the letter of _____,
pages _____, filed with the letter of _____.

☒ the claims, Nos. _____, as originally filed,
Nos. _____, as amended under Article 19,
Nos. _____, filed with the demand,
Nos. 1-18, filed with the letter of 20 December 2000 (20.12.2000),
Nos. _____, filed with the letter of _____.

☒ the drawings, sheets/fig 1/3-3/3, as originally filed,
sheets/fig _____, filed with the demand,
sheets/fig _____, filed with the letter of _____,
sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

☐ the description, pages _____

☐ the claims, Nos. _____

☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/EP 99/10141

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement**1. Statement**

Novelty (N)	Claims	2, 5-18	YES
	Claims	1, 3, 4	NO
Inventive step (IS)	Claims	9-18	YES
	Claims	1-8	NO
Industrial applicability (IA)	Claims	1-18	YES
	Claims		NO

2. Citations and explanations

Document US-A-3 833 796 (D1), which is regarded as the closest prior art, discloses (see abstract; column 2, line 17 to column 4, line 35) a document (10) with two six-figure numbers situated side by side. Of course it is also possible to read these two six-figure numbers as three four-figure numbers, the first being called "identification character", the second "document number" and the third "control number". In this manner, the document according to D1 has an at least machine-readable document number on the substrate and a storage field (the location where the third number is printed) for receiving the control number that is machine readable, an optical marking with the machine-readable identification character being placed on the substrate.

The subject matter of Claim 1 does not differ from that of this prior art document (see also Box VIII).

Therefore, the subject matter of Claim 1 is not novel (PCT Article 33(2)).

Dependent Claims 2-8 contain no additional features which, combined with the features of any claim to which they refer, meet the PCT requirements for novelty and inventive

step. The reasons are as follows:

The additional feature of Claim 2 is only one of several obvious possibilities from which a person skilled in the art would choose in order to solve the problem of interest, without thereby being inventive.

A check according to D1 must also have the additional features of Claims 3 and 4.

The additional features of Claims 5-8 are only one of several obvious possibilities from which a person skilled in the art would choose according to the circumstances in order to store data in a security document, without thereby being inventive.

Document D1, which is regarded as the closest prior art, discloses (see abstract; column 2, line 17 to column 4, line 35) a system from which the subject matter of Claim 9 differs at least in that the system contains a validation device, a calculating unit being contained therein for cryptographic operations with a first secret code for producing a control number by encoding at least two parameters--the document number and the identification character--and a recording means for entering the control number in the at least machine-readable storage field.

Therefore, the subject matter of Claim 9 is not novel (PCT Article 33(2)).

The problem addressed by the present invention can be regarded as creating the possibility to secure a document produced in large quantities such that its authenticity characteristics are not realized until the document is put into circulation so that theft no longer represents a

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/EP 99/10141

problem during the time period from production to presentation to the authorized person. The solution suggested to this problem in the present Claim 9 involves an inventive step for the following reasons (PCT Article 33(3)):

There is no indication of the differentiating features in the available prior art.

Claims 10-18 are dependent on Claim 9 and therefore likewise fulfil PCT requirements for novelty and inventive step.

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

Claim 9 lacks clarity for the following reason:

According to Claim 1, the document is fully realized when the control number is entered into the storage field. Accordingly, the features of Claim 9 pertaining to the validation device are useless (since the document is already validated). Hence, the system according to Claim 9 should have consisted of a document without a control number.

The feature in device Claim 1

that the control number is first placed in the storage field when the document is put into circulation pertains to a method of using the device and not to the definition of the device using its technical features. Contrary to the requirements of PCT Article 6, the intended limitations do not follow clearly from the claim. The above-mentioned feature is therefore not considered in assessing novelty and inventive step (see Box V above).

Furthermore, the feature that the control number is the result of a cryptographic operation with at least two parameters--the document number and the identification character--and a first secret code does not characterize the subject matter of Claim 1 since it can not be seen from one number on one individual document (as claimed) whether said number does or does not result from such a cryptographic operation since an arbitrary number can be produced through any cryptographic code. Similar considerations apply to the "identification character" and

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/EP 99/10141

VIII. Certain observations on the international application

the "document number" because only one single document is claimed. Hence, each of these features means nothing more than "number" (see Box V above).

The wording of the following (amended Claim 1, lines 5-10) is not grammatically correct in the German: "...that to activate a certificate of authenticity..." Furthermore, it remains unclear what the certificate of authenticity is and how it relates to the claimed document.

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT
AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts P2900W0	WEITERES VORGEHEN siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5	
Internationales Aktenzeichen PCT/EP 99/ 10141	Internationales Anmeldedatum (Tag/Monat/Jahr) 20/12/1999	(Frühestes) Prioritätsdatum (Tag/Monat/Jahr) 24/12/1998
Anmelder OVD KINEGRAM AG et al		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 2 Blätter.

☒ Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. Grundlage des Berichts

a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

☐ Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das

☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.

☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

☐ Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. ☐ Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen (siehe Feld I).

3. ☐ Mangelnde Einheitlichkeit der Erfindung (siehe Feld II).

4. Hinsichtlich der **Bezeichnung der Erfindung**

☒ wird der vom Anmelder eingereichte Wortlaut genehmigt.

☐ wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der **Zusammenfassung**

☒ wird der vom Anmelder eingereichte Wortlaut genehmigt.

☐ wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. 2

☒ wie vom Anmelder vorgeschlagen

☐ weil der Anmelder selbst keine Abbildung vorgeschlagen hat.

☐ weil diese Abbildung die Erfindung besser kennzeichnet.

☐ keine der Abb.

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 B42D15/10

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 B42D

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	US 3 833 795 A (SHOSHANI ET AL) 3. September 1974 (1974-09-03) in der Anmeldung erwähnt das ganze Dokument	1,8
A	EP 0 718 795 A (LANDIS & GYR TECHNOLOGY INNOVATION) 26. Juni 1996 (1996-06-26) in der Anmeldung erwähnt das ganze Dokument	1,8



Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen



Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann nahelegend ist

"Z" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

12. April 2000

Absendedatum des internationalen Recherchenberichts

25/04/2000

Name und Postanschrift der Internationalen Recherchenbehörde

Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Evans, A

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP 99/10141

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 3833795 A	03-09-1974	IL 37456 A	15-10-1975
		DE 2237911 A	01-03-1973
		FR 2149863 A	30-03-1973
		JP 48026346 A	06-04-1973
		NL 7210717 A	07-02-1973
<hr/>			
EP 718795 A	26-06-1996	CN 1157972 A	27-08-1997
		FI 956186 A	23-06-1996
		JP 8263841 A	11-10-1996
		NO 955158 A	24-06-1996
<hr/>			

Der Antrag ist bei der zuständigen mit der internationalen vorläufigen Prüfung beauftragten Behörde oder, wenn eine oder mehrere Behörden zuständig sind, bei der vom Anmelder gewählten Behörde einzureichen. Der Anmelder kann den Namen oder den Zweibuchstaben-Code der Behörde auf der nachstehenden Zeile angeben.

IPEA/ EP

PCT

KAPITEL II

ANTRAG AUF INTERNATIONALE VORLÄUFIGE PRÜFUNG

nach Artikel 31 des Vertrags über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens:
Der (die) Unterzeichnete(n) beantragt (beantragen), daß für die nachstehend bezeichnete internationale Anmeldung die internationale vorläufige Prüfung nach dem Vertrag über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens durchgeführt wird und benennt hiermit als ausgewählte Staaten
alle auswählbaren Staaten (soweit nichts anderes angegeben).

Von der mit der internationalen vorläufigen Prüfung beauftragten Behörde auszufüllen

Bezeichnung der IPEA	Eingangsdatum des ANTRAGS
----------------------	---------------------------

Feld Nr. I KENNZEICHNUNG DER INTERNATIONALEN ANMELDUNG		Aktenzeichen des Anmelders oder Anwalts T 2900W0/hs
Internationales Aktenzeichen PCT/EP99/10141	Internationales Anmeldedatum (Tag/Monat/Jahr) 20-12-1999 20. Dezember 1999	(Frühester) Prioritätstag (Tag/Monat/Jahr) 24-12-1998 24. Dezember 1998
Bezeichnung der Erfindung Aktivierbares Dokument und System für aktivierbare Dokumente		
Feld Nr. II ANMELDER		
Name und Anschrift: (Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben.) _OVD Kinegram AG Gubelstrasse 22 CH-6301 Zug Schweiz		Telefonnr.: Telefaxnr.: Fernschreibnr.:
Staatsangehörigkeit (Staat): CH	Sitz oder Wohnsitz (Staat): CH	
Name und Anschrift: (Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben.) TOMPKIN Wayne Robert Oesterliwaldweg 2 CH-5400 Baden Schweiz		
Staatsangehörigkeit (Staat): USA/CH	Sitz oder Wohnsitz (Staat): CH	
Name und Anschrift: (Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben.) STAUB René Schmiedstrasse 6 CH-6330 Cham Schweiz		
Staatsangehörigkeit (Staat): CH	Sitz oder Wohnsitz (Staat): CH	
<input type="checkbox"/> Weitere Anmelder sind auf einem Fortsetzungsblatt angegeben.		

Feld Nr. III ANWALT ODER GEMEINSAMER VERTRETER; ODER ZUSTELLANSCHRIFT

Die folgende Person ist ☒ Anwalt ☐ gemeinsamer Vertreter
 und ☒ ist vom (von den) Anmelder(n) bereits früher bestellt worden und vertritt ihn (sie) auch für die internationale vorläufige Prüfung.
☐ wird hiermit bestellt: eine etwaige frühere Bestellung eines Anwalts/gemeinsamen Vertreters wird hiermit widerrufen.
☐ wird hiermit zusätzlich zu dem bereits früher bestellten Anwalt/gemeinsamen Vertreter, nur für das Verfahren vor der mit der internationalen vorläufigen Prüfung beauftragten Behörde bestellt.

Name und Anschrift: (Familienname, Vorname: bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben.)

PÖHLAU Claus
 Louis, Pöhlau, Lohrentz & Segeth
 Postfach 30 55
 DE-90014 Nürnberg
 Deutschland

Telefonnr.:

0911/ 510 360

Telefaxnr.:

0911/ 511 342

Fernschreibnr.:

☐ **Zustellanschrift:** Dieses Kästchen ist anzukreuzen, wenn kein Anwalt oder gemeinsamer Vertreter bestellt ist und statt dessen im obigen Feld eine spezielle Zustellanschrift angegeben wird.

Feld Nr. IV GRUNDLAGE DER INTERNATIONALEN VORLÄUFIGEN PRÜFUNG

Erklärung betreffend Änderungen:*

1. Der Anmelder wünscht, daß die internationale vorläufige Prüfung auf der Grundlage

- ☒ der internationalen Anmeldung in der ursprünglich eingereichten Fassung
 der Beschreibung ☐ in der ursprünglich eingereichten Fassung
☐ unter Berücksichtigung der Änderungen nach Artikel 34
 der Patentansprüche ☐ in der ursprünglich eingereichten Fassung
☐ unter Berücksichtigung der Änderungen nach Artikel 19 (ggf. zusammen mit Begleitschreiben)
☐ unter Berücksichtigung der Änderungen nach Artikel 34
 der Zeichnungen ☐ in der ursprünglich eingereichten Fassung
☐ unter Berücksichtigung der Änderungen nach Artikel 34
 aufgenommen wird.

2. ☐ Der Anmelder wünscht, daß jegliche nach Artikel 19 eingereichte Änderung der Ansprüche als überholt angesehen wird.

3. ☐ Der Anmelder wünscht, daß der Beginn der internationalen vorläufigen Prüfung bis zum Ablauf von 20 Monaten ab dem Prioritätsdatum **aufgeschoben** wird, sofern die mit der internationalen vorläufigen Prüfung beauftragte Behörde nicht eine Kopie nach Artikel 19 vorgenommener Änderungen oder eine Erklärung des Anmelders erhält, daß er keine solchen Änderungen vornehmen will (Regel 69.1 Absatz d). (Dieses Kästchen darf nur angekreuzt werden, wenn die Frist nach Artikel 19 noch nicht abgelaufen ist.)

* Wenn kein Kästchen angekreuzt wird, wird mit der internationalen vorläufigen Prüfung auf der Grundlage der internationalen Anmeldung in der ursprünglich eingereichten Fassung begonnen: wenn eine Kopie der Änderungen nach Artikel 19 und/oder Änderungen der internationalen Anmeldung nach Artikel 34 bei der mit der internationalen vorläufigen Prüfung beauftragten Behörde eingeht, bevor diese mit der Erstellung eines schriftlichen Bescheids oder des internationalen vorläufigen Prüfungsberichts begonnen hat, wird jedoch die geänderte Fassung verwendet.

Sprache für die Zwecke der internationalen vorläufigen Prüfung: Deutsch ;

- ☒ dies ist die Sprache, in der die internationale Anmeldung eingereicht wurde.
☐ dies ist die Sprache der Übersetzung, die für die Zwecke der internationalen Recherche eingereicht wurde.
☐ dies ist die Sprache der Veröffentlichung der internationalen Anmeldung.
☐ dies ist die Sprache der Übersetzung, die für die Zwecke der internationalen vorläufigen Prüfung eingereicht wurde/wird.

Feld Nr. V BENENNUNG VON STAATEN ALS AUSGEWÄHLTE STAATEN

Der Anmelder benennt hiermit als ausgewählte Staaten alle auswählbaren Staaten (das heißt, alle Staaten, die bestimmt wurden und durch Kapitel II gebunden sind)
 mit Ausnahme der folgenden Staaten, die der Anmelder nicht benennen möchte:

Feld Nr. VI KONTROLLISTE

Dem Antrag liegen folgende Unterlagen für die Zwecke der internationalen vorläufigen Prüfung in der in Feld Nr. IV angegebenen Sprache bei:

- | | | |
|--|---|---------|
| 1. Übersetzung der internationalen Anmeldung | : | Blätter |
| 2. Änderungen nach Artikel 34 | : | Blätter |
| 3. Kopie (oder, falls erforderlich, Übersetzung) der Änderungen nach Artikel 19 | : | Blätter |
| 4. Kopie (oder, falls erforderlich, Übersetzung) einer Erklärung nach Artikel 19 | : | Blätter |
| 5. Begleitschreiben | : | Blätter |
| 6. Sonstige (einzeln auflühren) | : | Blätter |

Von der mit der internationalen vorläufigen Prüfung beauftragten Behörde auszufüllen

erhalten nicht erhalten

<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

Dem Antrag liegen außerdem die nachstehend angekreuzten Unterlagen bei:

- | | |
|--|---|
| 1. <input checked="" type="checkbox"/> Blatt für die Gebührenberechnung | 4. <input type="checkbox"/> Begründung für das Fehlen einer Unterschrift |
| 2. <input type="checkbox"/> unterzeichnete gesonderte Vollmacht | 5. <input type="checkbox"/> Nucleotid- und/oder Aminosäuresequenzprotokoll in computerlesbarer Form |
| 3. <input type="checkbox"/> Kopie der allgemeinen Vollmacht; Aktenzeichen (falls vorhanden): | 6. <input checked="" type="checkbox"/> sonstige (einzeln auflühren): Scheck |

Feld Nr. VII UNTERSCHRIFT DES ANMELDERS, ANWALTS ODER GEMEINSAMEN VERTRETERS

Der Name jeder unterzeichnenden Person ist neben der Unterschrift zu wiederholen, und es ist anzugeben, sofern sich dies nicht aus dem Antrag ergibt, in welcher Eigenschaft die Person unterzeichnet.

Nürnberg, 06.07.2000

W. Segeth, Patentanwalt

Von der mit der internationalen vorläufigen Prüfung beauftragten Behörde auszufüllen

- | | |
|--|---|
| 1. Datum des tatsächlichen Eingangs des ANTRAGS: | |
| 2. Geändertes Eingangsdatum des Antrags aufgrund von BERICHTIGUNGEN nach Regel 60.1 Absatz b: | |
| 3. <input type="checkbox"/> Eingangsdatum des Antrags NACH Ablauf von 19 Monaten ab Prioritätsdatum; Punkt 4 und Punkt 5, unten, finden keine Anwendung. | <input type="checkbox"/> Der Anmelder wurde entsprechend unterrichtet |
| 4. <input type="checkbox"/> Eingangsdatum des Antrags INNERHALB 19 Monate ab Prioritätsdatum wegen Fristverlängerung nach Regel 80.5. | |
| 5. <input type="checkbox"/> Das Eingangsdatum des Antrags liegt nach Ablauf von 19 Monaten ab Prioritätsdatum, der verspätete Eingang ist aber nach Regel 82 ENTSCHULDIGT. | |

Vom Internationalen Büro auszufüllen

Antrag vom IPEA erhalten am:

PATENTANSPRÜCHE

1. Dokument (1) mit einer wenigstens maschinell lesbaren Dokumentennummer (2) auf dem Substrat (6) und einem Speicherfeld (4) für die Aufnahme einer wenigstens maschinell lesbaren Kontrollnummer (9), dadurch gekennzeichnet, dass auf dem Substrat (6) eine optische Markierung (3) mit einer maschinell lesbaren Kennung (7) angebracht ist, und dass zur Aktivierung ein Echtheitszertifikat (23) die wenigstens maschinell lesbare Information im Speicherfeld (4) durch Einschreiben der das Ergebnis einer kryptographischen Operation mit wenigstens zwei Parametern, der Dokumentennummer (2) und der Kennung (7), und einem ersten geheimen Schlüssel (10) bildenden Kontrollnummer (9) in das Speicherfeld (4) erst bei der Inverkehrbringung vervollständigt ist.
2. Dokument (1) nach Anspruch 1, dadurch gekennzeichnet, dass die optische Markierung (3) beugungsoptische Strukturen aufweist, und dass wenigstens ein Teil der beugungsoptischen Strukturen die maschinell lesbare Kennung (7) enthält.
3. Dokument (1) nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass das Substrat (6) ein Kontrollfeld (5) für die Aufnahme eines wenigstens visuell lesbaren, individuellen und auf eine Person bezogenen Kodes (11) aufweist.
4. Dokument nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass das Speicherfeld (4) auf dem Substrat (6) angeordnet ist und dass nach der Aktivierung die Kontrollnummer (9) im Speicherfeld (4) in wenigstens maschinell lesbaren Zeichen enthalten ist.
5. Dokument (1) nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass im Substrat (6) ein Mikrochip (13) eingelassen ist, dass das Speicherfeld (4) im Speicher (14) des Mikrochips (13) angeordnet ist und dass nach der Aktivierung das Speicherfeld (4) die Kontrollnummer (9) enthält und der einmal eingeschriebene Inhalt des Speicherfelds (4) elektronisch nicht veränderbar ist.
6. Dokument (1) nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass auf dem Substrat (6) ein Magnetstreifen (16) mit dem Speicherfeld (4) angeordnet ist, dass der Magnetstreifen (16) wenigstens das Speicherfeld (4) enthält und dass nach der Aktivierung das Speicherfeld (4) die magnetisch lesbare Kontrollnummer (9) aufweist.
7. Dokument (1) nach Anspruch 1, 2, 3 oder 4, dadurch gekennzeichnet, dass auf dem Substrat (6) ein optischer Informationsträger (17, 17') angeordnet ist, dass der optische Informationsträger (17, 17') wenigstens das Speicherfeld (4) enthält und dass nach der Aktivierung der nicht mehr veränderbare optische Informationsträger (17, 17') im Speicherfeld (4) die Kontrollnummer (9) in optisch lesbaren Zeichen aufweist.
8. Dokument (1) nach Anspruch 7, dadurch gekennzeichnet, dass ein Teil des optischen Informationsträgers (17, 17') die optische Markierung (3) bildet und die Kennung (7) enthält.

9. System (20) bestehend aus wenigstens einem Dokument (1) nach einem der Ansprüche 1 bis 8, einem Validiergerät (21) und einem Verifikator (22),
dadurch gekennzeichnet,
dass im Validiergerät (21) eine Transportvorrichtung (25) zur Aufnahme des Dokuments (1), ein
5 Aufzeichnungsmittel (27) und ein optischer Leser (26) zum maschinellen Ablesen von wenigstens der
Kennung (7) angeordnet sind, dass das Validiergerät (21) weiter eine mit dem Aufzeichnungsmittel
(27) und dem optischen Leser (26) verbundene Recheneinheit (24) für kryptographische Operationen
mit einem ersten geheimen Schlüssel (10) zum Erzeugen der Kontrollnummer (9) durch Verschlüsseln
von wenigstens zwei Parametern, der Dokumentennummer (2) und der vom optischen Leser (26)
10 abgelesene Kennung (7), umfasst, dass das Aufzeichnungsmittel (27) zum Einschreiben der
Kontrollnummer (9) zum Aktivieren des Dokuments (1) zum Echtheitszertifikat (23) in das
wenigstens maschinell lesbare Speicherfeld (4) eingerichtet ist,
dass der Verifikator (22) wenigstens ein Rechengerät (33), einen optischen Leser (26) zum
maschinellen Ablesen der Kennung (7) und ein Aufnahmemittel (32) zum Ausrichten eines zu
15 überprüfenden Echtheitszertifikats (23) zum maschinellen Ablesen aufweist, dass das Rechengerät
(33) mit Eingabe- und Ablesemitteln (26; 28; 29) verbunden und für kryptographische Operationen
mit einem zweiten Schlüssel (34) sowie zur Überprüfung der Zusammengehörigkeit wenigstens der
Kontrollnummer (9) und der zum Verschlüsseln benutzten Parametern der kryptographischen
Operation, die auf dem Echtheitszertifikat (23) enthalten sind, und zur Darstellung des
20 Vergleichsergebnisses auf einer Anzeige (31) des Verifikators (22) und/oder zur Erzeugung eines
Erlaubnissignals eingerichtet ist.
10. System (20) nach Anspruch 9, dadurch gekennzeichnet, dass der Verifikator (22) eine
Tastatur (28) für eine manuelle Eingabe einer persönlichen Identifikationsnummer (PIN) zur Freigabe
des Verifikators (22) aufweist und dass der Verifikator (22) zum Überprüfen der persönlichen
25 Identifikationsnummer des Benutzers eingerichtet ist.
11. System (20) nach Anspruch 9 oder 10, dadurch gekennzeichnet, dass der Verifikator (22) eine mit
dem Rechengerät (33) verbundene Tastatur (28) für eine manuelle Eingabe der Parameter der
kryptographischen Operation an das Rechengerät (33) aufweist, wobei die Parameter wenigstens die
Dokumentennummer (2) und die Kontrollnummer (9) umfassen.
- 30 12. System (20) nach einem der Ansprüche 9 oder 11, dadurch gekennzeichnet, dass der
Verifikator (22) wenigstens eine mit dem Rechengerät (33) verbundene Leseinheit (29) für eine
maschinelle Eingabe der Parameter der kryptographischen Operation an das Rechengerät (33)
aufweist, wobei die Parameter wenigstens die Dokumentennummer (2) und die Kontrollnummer (9)
umfassen.

13. System (20) nach einem der Ansprüche 9 bis 12, dadurch gekennzeichnet, dass das Validiergerät (21) eine mit der Recheneinheit (24) verbundene Tastatur (28) für eine manuelle Eingabe wenigstens der Dokumentennummer (2) an die Recheneinheit (24) aufweist.
14. System (20) nach einem der Ansprüche 9 bis 12, dadurch gekennzeichnet, dass das Validiergerät (21) eine mit der Recheneinheit (24) verbundene Leseinheit (29) für eine maschinelle Eingabe der Dokumentennummer (2) an die Recheneinheit (24) aufweist.
15. System (20) nach einem der Ansprüche 9 bis 14, dadurch gekennzeichnet, dass das Validiergerät (21) für die Eingabe eines individuellen, auf eine berechnete Person bezogenen Codes (11) mittels einer Tastatur (28) eingerichtet ist, dass das Validiergerät (21) ein Aufzeichnungsmittel (27) im Validiergerät (21) zum Einschreiben des Codes (11) in das Kontrollfeld (5) umfasst und dass der Code (11) einer der Parameter für die Erzeugung der Kontrollnummer (9) im Validiergerät (21) bzw. für die Echtheitsprüfung im Verifikator (22) ist.
16. System (20) nach einem der Ansprüche 9 bis 15, dadurch gekennzeichnet, dass die Recheneinheit (24) im Validiergerät (21) derart ausgebildet ist, dass bei der Verschlüsselung der Kontrollnummer (9) eine über eine Tastatur (28) eingegebene persönlichen Identifikationsnummer der berechtigten Person als Parameter für die Erzeugung der Kontrollnummer (9) einbezogen ist und dass der Verifikator (22) das Erlaubnissignal nur dann im Rechenggerät (33) erzeugt, wenn bei der Echtheitsprüfung die persönlichen Identifikationsnummer über die Tastatur (28) des Verifikators (22) dem Rechenggerät (33) als Parameter der kryptographischen Operation einbezogen ist.
17. System (20) nach einem der Ansprüche 9 bis 16, dadurch gekennzeichnet, dass wenigstens ein Validiergerät (21) und wenigstens ein Verifikator (22) über ein Netzwerk (28', 38, 40; 37) mit einem zentralen Rechner (39) zum bidirektionalen Datenaustausch verbunden sind.
18. System (20) nach einem der Ansprüche 9 bis 17, dadurch gekennzeichnet, dass das wenigstens ein Verifikator (22) über eine Signalleitung (35) mit einer Dienstleistungseinrichtung (36) verbunden ist und dass die Dienstleistungseinrichtung (36) zum Freigeben einer Dienstleistung mittels des über die Signalleitung (35) an die Dienstleistungseinrichtung (36) gesandten Erlaubnissignals eingerichtet ist.

IN THE UNITED STATES PATENT AND TRADE MARK OFFICE

VERIFICATION OF TRANSLATION

I, Michael Wallace Richard Turner, Bachelor of Arts, Chartered Patent Attorney, European Patent Attorney, of 1 Horsefair Mews, Romsey, Hampshire SO51 8JG, England, do hereby declare that I am conversant with the English and German languages and that I am a competent translator thereof;

I verify that the attached English translation is a true and correct translation made by me of the attached Amended Pages in the German language of International Application PCT/EP99/10141;

I further declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment or both under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Date: June 14, 2001

MWR Turner
M W R Turner

CLAIMS

1. A document (1) having an at least machine-readable document number (2) on the substrate (6) and a storage field (4) for receiving a check number (9), characterised in that an optical marking (3) with a machine-readable identification (7) is disposed on the substrate (6), that the storage field (4) is adapted to receive the at least machine-readable check number (9), and that the check number (9) which is the result of a cryptographic operation with at least two parameters, the document number (2) and the identification (7), and a first secret key (10), is inserted in the storage field (4) for completion only when the document is brought into circulation as an authenticity certificate (23).

2. A document (1) as set forth in claim 1 characterised in that the optical marking (2) has optical-diffraction structures and that at least a part of the optical-diffraction structures includes the machine-readable identification (7).

3. A document (1) as set forth in claim 1 or claim 2 characterised in that the substrate (6) has a check field (5) for receiving an at least visually readable, individual code (11) which is related to a person.

4. A document as set forth in claim 1, claim 2 or claim 3 characterised in that the storage field (4) is arranged on the substrate (6) and that after activation the check number (9) is contained in the storage field (4) in at least machine-readable characters.

5. A document (1) as set forth in claim 1, claim 2, claim 3 or claim 4 characterised in that a microchip (13) is let into the substrate (6), that the storage field (4) is arranged in the memory (14) of the microchip (13), and that after activation the storage field (4) contains the check number (9) and the content of the storage field (4), once written in, cannot be altered electronically.

6. A document (1) as set forth in claim 1, claim 2, claim 3 or claim 4 characterised in that a magnetic strip (16) with the storage field (4) is arranged on the substrate (6), that the magnetic strip (16) contains at least the storage field (4), and that after activation the storage field (4) has the magnetically readable check number (9).

7. A document (1) as set forth in claim 1, claim 2, claim 3 or claim 4 characterised in that arranged on the substrate (6) is an optical information carrier (17, 17'), that the optical information carrier (17, 17') contains at least the storage field (4), and that after activation the optical information carrier (17, 17'') which can no longer be altered in the storage field (4) has the check number (9) in optically readable characters.

8. A document (1) as set forth in one of claims 1 through 7 characterised in that a part of the optical information carrier (17, 17') forms the optical marking (3) and contains the identification (7).

9. A system (20) comprising at least one document (1) as set forth in one of claims 1 through 8, a validation device (21) and a verifier (22), characterised in that the document (1) has at least one machine-readable document number (2), an optical marking (3) with a machine-readable identification (7), and an at least machine-readable storage field (4) for receiving a check number (9),

that arranged in the validation device (21) are a receiving device (25) for receiving the document (1) and an optical reader (26) for machine reading of at least the identification (7), that provided in the validation device (21) is a computing unit (24) for cryptographic operations with a first secret key (10) for producing the check number (9) by encryption of at least two parameters, the document number (2) and the identification (7), that a recording means (27) is adapted to write the check number (9) into the at least machine-readable storage field (4),

that the verifier (22) has at least a computing unit (33), an optical reader (26) for machine reading of the identification (7), and a receiving means (32) for orienting an authenticity certificate (23) for the machine reading operation, that the verifier (22) includes the computing unit (33) connected at least to input and reading-off means (26; 28; 29) for cryptographic operations with a second key (34), and that the computing unit (33) is adapted to check the relatedness at least of the check number (9) and the parameters of the cryptographic operation, which are used for the encryption procedure and which are contained on the authenticity certificate (23), and to represent the comparison result on a display (31) of the verifier (22) and/or to produce a permission signal.

10. A system (20) as set forth in claim 9 characterised in that the verifier (22) has a keyboard (28) for manual input of a personal identification number (PIN) for enablement of the verifier (22) and that the verifier (22) is adapted to check the personal identification number.

11. A system (20) as set forth in claim 9 or claim 10 characterised in that the verifier (22) has a keyboard (28) connected to the computing unit (33) for manual input at least of the document number (2) and the check number (9) to the computing unit (33).

12. A system (20) as set forth in one of claims 9 through 11 characterised in that the verifier (22) has at least one reading unit (29) connected to the computing unit (33) for manual input of the document number (2) and the check number (9) to the computing unit (33).

13. A system (20) as set forth in claim 9 characterised in that the validation device (21) has a keyboard (28) connected to the computing unit (24) for manual input at least of the document number to the computing unit (24).

14. A system (20) as set forth in claim 9 or claim 13 characterised in that the validation device (21) has a reading unit (29) connected to the computing unit (24) for manual input at least of the document number (2) to the computing unit (24).

15. A system (20) as set forth in claim 9, claim 13 or claim 14 characterised in that the validation device (21) is adapted for the input of an individual code (11) related to a person, by means of the keyboard (21), and that the recording means (27) is arranged in the validation device (21) for writing the code (11) into the check field (5).

16. A system (20) as set forth in one of claims 9 through 15 characterised in that the computing unit (24) in the validation device (21) is such that upon encryption of the check number (9) a personal identification number of the authorised person which is inputted by way of a keyboard (28) is incorporated as a parameter for production of the check number (9) and that the verifier (22) produces the permission signal in the computing unit (33) only when in the authenticity checking procedure the personal identification number is incorporated by way of the keyboard (28) of the verifier (22) in the computing unit (33) as a parameter of the cryptographic operation.

17. A system (20) as set forth in one of claims 9 through 16 characterised in that at least one validation device (21) and at least one verifier (22) are connected by way of a network (28', 38, 40; 37) to a central computer (39) for bidirectional data exchange.

18. A system (20) as set forth in one of claims 9 through 17 characterised in that the at least one verifier (22) is connected by way of a signal line (35) to a service apparatus (36) and that the service apparatus (36) is adapted to enable a service by means of the permission signal sent to the service apparatus (36) by way of the signal line (35).

IN THE UNITED STATES PATENT AND TRADE MARK OFFICE

VERIFICATION OF TRANSLATION

I, Michael Wallace Richard Turner, Bachelor of Arts, Chartered Patent Attorney, European Patent Attorney, of 1 Horsefair Mews, Romsey, Hampshire SO51 8JG, England, do hereby declare that I am conversant with the English and German languages and that I am a competent translator thereof;

I verify that the attached English translation is a true and correct translation made by me of the attached specification in the German language of International Application PCT/EP99/10141;

I further declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment or both under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Date: June 14, 2001



M W R Turner

Aktivierbares Dokument und System für aktivierbare Dokumente

Die Erfindung bezieht sich auf ein aktivierbares Dokument gemäss dem Oberbegriff des Anspruchs 1 und auf ein System für aktivierbare Dokumente gemäss dem Oberbegriff des Anspruchs 9.

Solche aktivierbare Dokumente sind für persönliche Ausweise verwendbar, wie z.B. Bankschecks, Pässe, Identitätskarten, Abonnements, Billette, Gesundheitskarten, Kreditkarten, IC-Karten, elektronische Geldbörsen, (smart cards), Wertdokumente usw. Ein solches System, das aktivierbare Dokumente verwendet, sind vor allem bei Echtheitskontrollen und/oder Inhaber - Kontrollen der Dokumente verwendbar.

Zur Sicherung der genannten Dokumente werden visuell leicht erkennbare Hologramme und andere Beugungsstrukturen eingesetzt, wobei sie meist in Form von Etiketten aus einem die beugungsoptisch wirksamen Strukturen schützenden Kunststofflaminat mit dem Substrat des Dokuments unlösbar verbunden sind (EP 0 330 738 A1). An und für weisen solche Dokumente einen sehr hohen Sicherheitsstandard gegen Fälschungen oder Verfälschungen auf.

Aus der EP 0 713 197 A1 ist ein Datenträger in Kartenform mit einer in den Kartenkörper integrierten elektronischen Schaltung und einer optischen Markierung bekannt, wobei der Inhalt der elektronischen Schaltung mit der Information der optischen Markierung verknüpft ist. Als optische Markierungen können beispielsweise mit Farbe aufgebrachte Zeichen, wie ein Barcode oder Schriftzeichen, oder beugungsoptisch wirksame Strukturen, wie sie in der CH -PS 653 161 A5, in der EP 0 366 858 A1, in der EP 0 718 795 A1, in der EP 0 883 085 A1 usw. verwendet werden. In den genannten Schriften sind auch Ausführungen von Lese- und Schreibgeräten für die optischen Markierungen beschrieben.

Schliesslich beschreibt die US -PS 3 833 795 die Sicherung der Echtheit von seriell nummerierten Dokumenten (Banknoten, Wertpapiere). Eine solches Dokument trägt zwei Nummernfelder, das eine ist für eine fortlaufende Nummerierung der Dokumente, der Identitätsnummer, vorgesehen, das andere ist eine bei der Ausgabe zufällig gewählte Kontrollnummer, die in eine zentral geführte Liste eingetragen wird. Ein ausgegebenes Dokument wird anhand der externen Liste oder mittels eines Listen - Algorithmus überprüft, wobei eine Leseeinrichtung zunächst die Identitätsnummer und die Kontrollnummer abliest und anschliessend die Kontrollnummer der Identitätsnummer auf dem Dokument mit der von der Leseeinrichtung mittels der externen Liste oder des Listen-Algorithmus gefundenen Kontrollnummer vergleicht. Dieses Dokument ist jedoch nicht gegen Kopieren geschützt.

Ein grosses Problem stellt jedoch die Sicherheit der Dokumente im Zeitraum von der Herstellung bis zur Übergabe des Dokuments an die berechtigte Person dar, da in diesem Zeitraum die Dokumente auf dem Transport gestohlen werden können, um mit diesen Dokumenten unberechtigte Personen auszurüsten.

Der Erfindung liegt die Aufgabe zugrunde, ein in grossen Mengen kostengünstig hergestelltes, gegen Kopieren geschütztes Dokument derart zu sichern, dass seine Echtheitsmerkmale erst beim Inverkehrbringen vervollständigt werden und die Echtheitsmerkmale einfach und kostengünstig maschinell zu überprüfen sind.

Die genannte Aufgabe wird erfindungsgemäss durch die im Kennzeichen der Ansprüche 1 und 9 angegebenen Merkmale gelöst. Vorteilhafte Ausgestaltungen der Erfindung ergeben sich aus den abhängigen Ansprüchen.

Ausführungsbeispiele der Erfindung sind in der Zeichnung dargestellt und werden im folgenden näher beschrieben.

Es zeigen:

Figur 1	ein Dokument,
Figur 2	ein aktiviertes Dokument,
Figur 3	eine IC -Karte als Dokument,
Figur 4	einen Informationsstreifen,
Figur 5	ein System,
Figur 6	ein Validiergerät und
Figur 7	einen Verifikator.

In der Figur 1 bedeutet 1 ein Dokument, 2 Dokumentennummer, 3 eine optische Markierung, 4 ein Speicherfeld, 5 ein Kontrollfeld und 6 ein Substrat. Das Dokument 1 besitzt ein Substrat 6 aus Papier, Kunststoffvlies, Kunststoffolie, einem Schichtverbund aus Kunststoff, Lacken und/oder Papier usw. Die beiden Oberflächen des Substrats 6 können bedruckt sein, wie dies bei Bankschecks, Pässen, Identitätskarten, Abonnements, Billetts, Gesundheitskarten, Kreditkarten, IC-Karten, elektronische Geldbörsen (smart cards), Wertdokumente, Banknoten usw. üblich ist, und weisen wenigstens auf einer Seite die wenigstens maschinell lesbare Dokumentennummer 2 auf. Die Dokumentennummer 2 kann in Klarschrift und/oder als Strichkode in bekannter Art mit normaler, fluoreszierender oder magnetischer Tinte auf das Substrat 6 aufgebracht sein. Für die optische Markierung 3 sind beispielsweise mit normaler, fluoreszierender oder magnetischer Farbe aufgebrachte oder mittels Perforieren des Substrats 6 erzeugte Zeichen, wie ein Barcode, Schriftzeichen usw., oder beugungsoptisch wirksame Strukturen verwendbar. Die optische Markierung 3 enthält eine digitale Information, eine Kennung 7. Von besonderem Vorteil ist die Verwendung der optischen Markierung 3 mit beugungsoptisch wirksamen Strukturen wegen ihrer hohen Sicherheit gegen Fälschung und Kopieren, Sie sind aus den eingangs genannten Schriften CH 653 161 A5, EP 0 366 858 A1, EP 0 7 18 795 A1 usw. bekannt und eignen sich besonders zum maschinellen Ablesen einer in der beugungsoptischen Markierung 3

enthaltenen Kennung 7. Die Kennung 7 beinhaltet Informationen über die Art des Dokuments, die Dokumentserie usw. nicht aber über die Dokumentennummer 2, die das Dokument 1 innerhalb einer Serie identifiziert, d.h. die Dokumente 1 einer Serie sind kostengünstig herstellbar und unterscheiden sich nur durch die beispielsweise aufgedruckten Dokumentennummern 2. Die Grösse der optischen Markierung 3 ist durch die darin enthaltene Kennung 7 bestimmt und die benötigte Fläche umfasst typisch ungefähr 1 mm^2 . Extremwerte für diese Fläche dürften bei $0,1 \text{ mm}^2$ eine untere und bei 1 cm^2 eine obere Grenze erreichen. Die optische Markierung 3 kann auch visuell unsichtbar in einer transparenten Folie gemäss CH 653 161 A5 eingebracht sein oder auch unauffällig innerhalb eines Hologramms oder eines beugungsoptischen Musters, einem Sicherheitsmerkmal 8, beispielsweise gemäss CH 659 433 A5, verborgen sein. Das Sicherheitsmerkmal 8 dient der Identifizierung des Dokuments 1 für den Mann auf der Strasse und wirkt auf dem Dokument 1 sehr auffällig.

Das Speicherfeld 4 und das Kontrollfeld 5 bleiben zur Auslieferung an die Inverkehrbringer (Verkaufsstellen, Ausgabestellen, Bankschalter usw.) leer. Ohne eine in der Figur 2 gezeigte Kontrollnummer 9 im Speicherfeld 4 ist das Dokument 1 unbrauchbar. Beim Inverkehrbringen müssen die Dokumente 1 durch eine Aktivierung ihre Gültigkeit erlangen. Beispielsweise werden die Dokumentennummer 2 und die Kennung 7 maschinell aus dem Dokument 1 abgelesen. Wenigstens diese Informationen werden mit einem ausserhalb des Dokuments vorhandenen ersten geheimen Schlüssel 10 in einer kryptographischen Operation miteinander verknüpft und aus dem Resultat die dem Dokument 1 zugehörige Kontrollnummer 9 erzeugt und in das Speicherfeld 4 eingeschrieben. Das Dokument 1 ist erst jetzt vollständig und seine Gültigkeit ist anhand der Dokumentennummer 2, der Kennung 7 und der Kontrollnummer 9 überprüfbar. Bei bestimmten Dokumentarten ist während der Aktivierung auch die Beschriftung des Kontrollfelds 5 vorgesehen. Der Inhalt des Kontrollfelds 5 umfasst wenigstens visuell lesbare, individuelle, auf eine Person, Veranstaltung, Firma, usw. bezogene Informationen, wie Name, Anschrift, Sozial- oder andere Versicherungsnummer, Staatszugehörigkeit, Zeitangaben, Geldbetrag usw. Diese Informationen, im folgenden Kode 11 genannt, können auch zusammen mit der Dokumentennummer 2, der Kennung 7 mit der kryptographischen Operation zur Kontrollnummer 9 verarbeitet werden.

In einer Ausführung des Dokuments 1 ist nach einem der bekannten Verfahren das Speicherfeld 4 und/oder das Kontrollfeld 5 mit der Kontrollnummer 9 bzw., dem Kode 11 in maschinenlesbarer Druckschrift beschriftet. Diese Klarschrift, z.B. OCR -Schrift, ist sowohl visuell als auch maschinell lesbar. Anstelle oder zusammen mit der Druckschrift kann die Kontrollnummer 9 auch als Strichkode, der im Detailhandel weit verbreitet ist, dargestellt sein.

In der Figur 3 ist eine weitere Ausführung des Dokuments 1 in Form einer Karte (Gesundheitskarte, Kreditkarte, IC-Karte, Smartcards, usw) gezeigt. In das Substrat 6 ist ein an sich bekanntes Modul 12

mit einem der Mikrochip 13 eingelassen, in dessen Speicher 14 das Speicherfeld 4 eingerichtet ist. Das Speicherfeld 4 kann nur einmal mit der Kontrollnummer 9 beim Aktivieren des Dokuments 1 mittels einer über ein Kontaktfeld 15 gesandte elektronischen Signalfolge beschrieben werden, eine spätere Veränderung ist nicht mehr möglich. Wie in der eingangs erwähnten EP 0 713 197 A1 kann die Signalfolge auch mittels hier nicht gezeigten induktiven oder optischen Mitteln an ein entsprechend gestaltetes Modul 12 des Dokuments 1 übertragen werden.

Eine andere Ausführung des Dokuments 1 in Kartenform weist auf dem Substrat 7 einen Magnetstreifen 16 auf. Die Kontrollnummer 9 (Figur 2) und der Kode 11 (Figur 2) wird beim Aktivieren des Dokuments 1 magnetisch kodiert in das Speicherfeld 4 bzw. in das Kodierfeld 5 auf dem Magnetstreifen 16 eingezeichnet. Das Speicherfeld 4 weist nach der Aktivierung im Speicherfeld 4 wenigstens die magnetisch lesbare Kontrollnummer 9 auf.

Eine weitere Ausführung des Dokuments 1 weist im Speicherfeld 4 einen mit dem Substrat 6 während des Herstellungsprozesses des Dokuments 1 aufgebracht, in der Figur 4 dargestellten beugungsoptischen Informationsträger 17 auf, wie er in der eingangs genannten Schrift EP 0 718 795 A1 beschrieben ist. Der Informationsträger 17 weist im unbeschriebenen Zustand 17' wenigstens eine Reihe von in Paaren 19 angeordneten Beugungsfeldern 18, wobei sich die beiden mikroskopischen Beugungsstrukturen eines Paares 19 in wenigstens einem Gitterparameter unterscheiden. Während des Aktivierens wird die Kontrollnummer 9 als digitale Folge auf dem Informationsträger 17 abgebildet, wobei beim Beschreiben entsprechend dem Bitwert in jedem Paar eines der beiden Beugungsfelder 18 die Beugungsstruktur durch Zuführen von Wärmeenergie zerstört oder die Beugungsstruktur durch Abdecken, z.B. mit einem nicht transparenten Decklack, unwirksam gemacht wird. Im Informationsträger 17" ist nach der Aktivierung bei jedem Paar eine der beiden Beugungsstrukturen nicht mehr beugungsoptisch wirksam. Das Speicherfeld 4 weist nun die Kontrollnummer 9 in optisch maschinell leicht lesbaren Zeichen auf. Der Vorteil dieses Informationsträgers 17 ist, dass er nur einmal beschrieben werden kann. Jede weitere Veränderung des Informationsträgers 17 ist maschinell leicht zu erkennen.

In einer Ausführung des Dokuments 1 ist die optische Markierung 3 und die Kontrollnummer 9 mit Beugungsstrukturen ausgeführt und auf dem gleichen Informationsträger 17 untergebracht. Der Vorteil dieser Ausführung ist, dass mit einem einzigen optischen Leser 26 gemäss der EP 0 718 795 A1 das Auslesen der Kennung 7 und der Kontrollnummer 9 sowie das Beschriften des Informationsträgers 17 durchgeführt wird. Das teure Sicherheitsmerkmal 8 (Figur 1) kann weggelassen werden.

Die Beschriftungen 2, 9, 11, das Modul 12 und der Magnetstreifen 16 können an sich beliebig auf den beiden Seiten des Dokuments 1 verteilt sein, wobei üblicherweise nur der Magnetstreifen 16 auf der Rückseite des Substrats 6 angeordnet ist.

Die Figur 5 zeigt ein System 20, das sich für die Verwendung der vorstehend beschriebenen Dokumente 1 eignet. Das System 20 umfasst wenigstens ein Dokument 1, ein Validiergerät 21 für die Aktivierung des Dokuments 1 und einen Verifikator 22, mit dem eine Echtheitskontrolle des Dokuments 1 durchzuführen ist. Während die Validiergeräte 21 bei den wenigen Inverkehrbringern aufgestellt sind, muss eine Vielzahl von einfach zu bedienenden, möglichst autonomen Verifikatoren 22 dort im Einsatz sein, wo auch immer solche Dokumente 1 einer Echtheitskontrolle unterzogen werden.

Die vom Hersteller angelieferten Dokumente 1 mit der Dokumentennummer 2 werden bei den Inverkehrbringern gelagert bis eines der Dokumente 1 einer berechtigten Person zugeteilt wird, wobei mittels des Validiergerätes 21 das dieser Person zugeteilte Dokument 1 durch Einschreiben der Kontrollnummer 9 in das Speicherfeld 4 zu einem Echtheitszertifikat 23 vervollständigt wird.

Eine Ausführung des Validiergeräts 21 gemäss Figur 6 umfasst eine Recheneinheit 24, eine Transportvorrichtung 25 für das Dokument 1, einen optischen Leser 26 zum maschinellen Auslesen der Kennung 7 (Figur 1) auf der optischen Markierung 3 des nicht aktivierten Dokuments 1 sowie ein Aufzeichnungsmittel 27. Weitere in der Zeichnung der Figur 6 gestrichelt eingezeichnete, fakultative Leseeinheiten 29 ermöglichen ein Ablesen der Dokumentennummer 2 (Figur 1), der Kontrollnummer 9 (Figur 2) und des Codes 11 (Figur 2). Die Leseeinheiten 29 unterscheiden sich entsprechend der für das System 20 einmal gewählten Aufzeichnungstechniken, die für die Dokumentennummer 2, für die Kontrollnummer 9 und für den Code 11 vorbestimmt sind. Die Transportvorrichtung 25, der optische Leser 26, das oder die Aufzeichnungsmittel 27 und die Leseeinheiten 29 sind mit der Recheneinheit 24 verbunden.

Die Recheneinheit 24 ist über Leitungen mit der Transportvorrichtung 25, dem optischen Leser 26, und mit dem Aufzeichnungsmittel 27 verbunden, steuert diese Geräte 25, 26, 27 und empfängt die von diesen Geräten 25, 26, 27 ausgesandte Informationen, damit das Dokument 1 maschinell abgelesen und beschriftet werden kann. Die Recheneinheit 24 weist wenigstens ein Sicherheitsmodul 30 auf, das in einer integrierte Schaltung einen Mikroprozessor mit zugehörigen Speicherplätzen umfasst. Der Mikroprozessor führt kryptographische Operationen aus und benutzt dazu den in den Speicherplätzen enthaltenen ersten geheimen Schlüssel 10.

Die Transportvorrichtung 25 bewirkt in einer Ausführung eine Relativbewegung zwischen dem Dokument 1 einerseits und den Lesemitteln 26, 29 und dem Aufzeichnungsmittel 27 andererseits. In der Figur 6 wird das Dokument 1 gegenüber den feststehenden Lesemitteln 26, 29 und dem Aufzeichnungsmittel 27 bewegt. Für die Transportvorrichtung 25 sind unterschiedliche, an sich bekannte Ausführungen für Blätter oder für Karten bekannt und einsetzbar. Auf eine aufwendige Transportvorrichtung 25 kann verzichtet werden, wenn die optische Markierung 3 bzw. das

Sicherheitselement 8 (Figur 1) gemäss der Lehre in der EP 0 883 085 A1 gestaltet ist und das Beschriften des Speicherfelds 4 manuell erfolgt.

Das Aufzeichnungsmittel 27 ist zum Einschreiben der Kontrollnummer 9 und des Codes 11 in das Speicherfeld 4 bzw. Kodierfeld 5 eingerichtet und benutzt die für das Dokument 1 vorgesehene Aufzeichnungstechnik, beispielsweise ein Druck-, Tintenstrahl-, Xerographie-, Perforations- usw. Verfahren, ein in der EP 0 718 795 A1 beschriebenes Schreibverfahren für die Informationsträger 17, eine magnetische Aufzeichnung oder die elektronische Speicherung im Speicher 14 (Figur 3). Die Kontrollnummer 9 kann auch manuell in das Speicherfeld 4 mit dokumentechter Tinte eingeschrieben werden. Das Perforationsverfahren für Dokumente 1 ist z.B. im DE Gebrauchsmuster G 93 15 294.9 beschrieben.

Die Tastatur 28 ist ganz allgemein eine Eingabevorrichtung für aus Ziffern oder alphanumerische Zeichen bestehende Informationen. Die Eingabevorrichtung kann auch über einen Anschluss 28' an ein Telefon- oder Computernetzwerk 37 (Figur 5) mit dem Validiergerät 21 verbunden sein, insbesondere können die den Kode 11 bildenden Informationen von einer Zentralstelle abgerufen werden.

Die Leseinheit 29 ist der für das Dokument 1 verwendeten Aufzeichnungstechnik angepasst. Die Leseinheit 29 ist z.B. ein Klarschriftleser, ein Barkodeleser usw. für visuell lesbare Zeichen, aus denen sich die Dokumentennummer 2, die Kontrollnummer 9 und den Kode 11 zusammensetzen. Diese Leseinheiten 29 tasten mit einem Lichtstrahl Teile oder das ganze Dokument 1 ab und messen die Intensität des vom Dokument 1 zurückgestreuten Lichts. Die für die magnetisch aufgezeichnete Informationen bzw. zum elektronischen Auslesen aus dem Speicher 14 geeignete Leseinheit 29 ist allgemein bekannt.

Der Aufbau und Arbeitsweise des optischen Lesers 26 und für eine Leseinheit 29, die zum Auslesen der Kontrollnummer 9 aus dem optischen Informationsträger 17 (Figur 4) befähigt ist, sind beispielsweise aus den eingangs genannten Schriften CH-PS 653 161 A5; EP 0 366 858 A1, EP 0 718 795 A1, EP 0 883'085 A1 bekannt.

In einer kostengünstigen Ausführung zur Aktivierung liest ein Bediensteter eines nicht aktivierten Dokuments 1 dessen Dokumentennummer 2 visuell ab und gibt die Dokumentennummer 2 (Figur 2) über eine Tastatur 28 manuell in die Recheneinheit 24 ein. Anschliessend wird das Dokument 1 in die auf einen Kanal oder eine Plattform reduzierte Transportvorrichtung 25 unter den optischen Leser 26 gesteckt bzw. gelegt, damit der optische Leser 26 die Kennung 7 ablesen und der Recheneinheit 24 übermitteln kann. Die Recheneinheit 24 verschlüsselt die Kennung 7 und die Dokumentennummer 2 mit dem ersten geheimen Schlüssels 10 und bildet eine digitale Signatur, die Kontrollnummer 9, auf einer Anzeige 31 ab. Der Bedienstete überträgt nun manuell die Kontrollnummer 9 in das Speicherfeld 4 auf dem Dokument 1, das nun derart aktiviert zum Echtheitszertifikat 23 (Figur 5) geworden ist. Das

Speicherfeld 4 kann in Felder für je ein Zeichen der Kontrollnummer 9 eingeteilt sein, um ein maschinelles Lesen der handschriftlich eingetragenen Kontrollnummer 9 zu erleichtern.

Eine zweite Ausführung weist eine in der Zeichnung der Figur 6 punktiert gezeichnete Lesereinheit 29 auf, die die Dokumentennummer 2 maschinell direkt vom Dokument 1 abliest und an die Recheneinheit 24 abgibt. Die Recheneinheit 24 verschlüsselt wenigstens die Kennung 7 und die Dokumentennummer 2 mit dem ersten geheimen Schlüssels 10 zur Kontrollnummer 9. Anschliessend überträgt das Aufzeichnungsmittel 27 die Kontrollnummer 9 in den Speicherfeld 4 in der vom System 20 vorbestimmten Technik.

Das Validiergerät 21 ist in einer dritten Ausführung zusätzlich mit der Tastatur 28 und der Anzeige 31 ausgestattet, um über die Tastatur 28 den Kode 11 einzugeben, wobei die Anzeige 31 zur Kontrolle des Kodes 11 dient. Der Kode 11 wird ebenfalls mit dem Aufzeichnungsmittel 27 auf das Dokument 1 übertragen. Für besonders wichtige Dokumente 1 ist das Validiergerät 21 dazu eingerichtet, die Eingabe einer persönlichen Identifikationsnummer (PIN) vom Benutzer zu verlangen. Diese PIN identifiziert in einem Fall als Zulassungs-PIN den Bediensteten, der das Validiergerät 21 bedient, und in einem zweiten Fall als Inhaber - PIN den Dokumentinhaber, wobei bei der Aktivierung des Dokuments 1 der Inhaber seine PIN über die Tastatur 28 eintippt und im Rechengerät 24 die Inhaber - PIN zusammen mit dem Kode 11 oder allein als Parameter für die Erzeugung der Kontrollnummer 9 dient.

In einer vierten Ausführung des Validiergeräts 21 ist anstelle des optischen Lesers 26 und der Leseinheit 29 ein einziger Leser 26 so eingerichtet, dass er sowohl die optische Markierung 3 und die Dokumentennummer 9 erkennen kann.

In einer fünften Ausführung ist das Validiergerät 21 auch zum Erkennen der Kontrollnummer 9 eingerichtet. Somit ist das Validiergerät 21 fähig, aktivierte und nicht aktivierte Dokumente 1 zu unterscheiden und zusätzlich die Kontrollnummer 9 auf ihre Richtigkeit zu überprüfen.

Die Kontrollnummer 9 ist das Ergebnis der kryptographischen Operation in der Recheneinheit 24, einer mathematischen Funktion f:

Kontrollnummer 9 = f(Dokumentennummer 2, Kennung 7, erster geheimer Schlüssel 10) bzw.

Kontrollnummer 9 = f(Dokumentennummer 2, Kennung 7, Kode 11, erster geheimer Schlüssel 10).

Da sich die Systeme 20 nicht nur in der Aufzeichnungstechnik sondern auch in der Anzahl und Art der Parameter der kryptographischen Operation unterscheiden, werden, zwecks einfacherer Beschreibung, nachfolgend die für die Erzeugung der Kontrollnummer 9 auf dem Dokument 1 vorhandenen Werte, wie Dokumentennummer 2, Kennung 7, Kode 11 und die getrennt vom Dokument 1 gespeicherte Inhaber- PIN, als Parameter der kryptographischen Operation bezeichnet, wobei darunter wenigstens die Dokumentennummer 2 und die Kennung 7 zu verstehen sind, allenfalls ergänzt um den Kode 11

und/oder die Inhaber -PIN. Ein System 20 ist somit durch die verwendeten Aufzeichnungstechniken, die Ausführung des Dokuments 1, die Parameter der kryptographischen Operation und dem ersten geheimen Schlüssel 10 bestimmt.

Weder der erste geheime Schlüssel 10 noch der Algorithmus sind der Öffentlichkeit bekannt und werden von einer "certification authority" in einem Sicherheitsmodul 30 zum Einsetzen in die Recheneinheit 23 abgegeben. Nachdem die Recheneinheit 24 die Parameter der Funktion f in das Sicherheitsmodul 30 eingegeben sind, erzeugt das leicht auswechselbare Sicherheitsmodul 30 direkt die Kontrollnummer 9 oder ein Zwischenresultat, das für die Berechnung der Kontrollnummer 9 in der Recheneinheit 24 dient.

Der erste geheime Schlüssel 10 dient sowohl für die kryptographischen Operation zum Erzeugen der Kontrollnummer 9 als auch für die Überprüfung der Richtigkeit der Kontrollnummer 9 in Kenntnis der auf dem Dokument 1 vorhandenen Informationen.

Der Verifikator 22 in der Figur 7 weist bis auf das Aufzeichnungsmittel 27 (Figur 6) gleiche Komponenten wie das Validiergerät 21 (Figur 6) auf. Die Ausführungen des Verifikator 22 unterscheiden sich in den Leseinheiten 29, die sich entsprechend der für das System 20 (Figur 5) gewählten Aufzeichnungstechnik unterscheiden. Der Verifikator 22 umfasst in der kostengünstigen Ausführung wenigstens ein Aufnahmemittel 32 für ein zu überprüfendes Echtheitszertifikat 23 (Figur 5), ein Rechengerät 33 mit dem Sicherheitsmodul 30, den optischen Leser 26 für die Kennung 7, die Tastatur 28 und die Anzeige 31. Das Rechengerät 33 ist mit dem optischen Leser 26, der Tastatur 28 und der Anzeige 31 verbunden. Das Rechengerät 33 überprüft mit einer anderen kryptographischen Operation, ob die Kontrollnummer 9 (Figur 2) zu den Parametern der kryptographischen Operation, die wenigstens die Dokumentnummer 2 und die Kennung 7 umfassen, passt. Dazu verwendet das Rechengerät 33 einen zweiten Schlüssel 34, der im Sicherheitsmodul 30 mit dem entsprechenden Algorithmus enthalten ist. Das Rechengerät 33 kann mit der anderen kryptographischen Operation keine Verschlüsselungen wie die Recheneinheit 24 (Figur 6) im Validiergerät 21 vornehmen. Die Verwendung des zweiten Schlüssels 34, der vom ersten Schlüssel 10 völlig verschieden ist, weist den Vorteil auf, dass die sich aus der Verwendung ergebenden weiten Verbreitung der Verifikatoren 22 ergebenden Schwierigkeit der Geheimhaltung des zweiten Schlüssels 34 für die Sicherheit des Systems 20 irrelevant ist. Das Rechengerät 32 stellt das Ergebnis der Echtheitskontrolle auf der Anzeige 31 dar.

Für eine Echtheitskontrolle liest ein Kontrolleur visuell die Parameter der kryptographischen Operation, wenigstens die Dokumentnummer 2 und die Kennung 7, auf dem Echtheitszertifikat 23 und die Kontrollnummer 9 im Speicherfeld 4 ab und führt dem Rechengerät 33 die abgelesenen Zeichenfolgen über die Tastatur 28 zu. Das Aufnahmemittel 32 kann auch eine einfache Plattform unter dem optischen Leser 26 sein, auf die der Kontrolleur das Dokument 1 so auflegt, dass die optische Markierung 3 im

Bereich des optischen Lesers 26 ist. Die maschinell gelesene Kennung 7 gelangt direkt in das Rechengerät 33. Das Ergebnis der Echtheitskontrolle erscheint auf der Anzeige 31. Im einfachsten Fall besteht die Anzeige 31 aus zwei Signallampen um das Ja/Nein -Ergebnis der Echtheitskontrolle darzustellen. Jedoch ist es von Vorteil, wenn die Anzeige 31 sowohl die über die Tastatur 28 eingegebenen Parameter und Kontrollzahl 9 sowie das Ja/Nein -Ergebnis anzeigt.

Der Verifikator 22 gibt in einer anderen Ausführung ein Erlaubnissignal über eine Signalleitung 35 an eine Dienstleistungseinrichtung 36 ab. Das Eintreffen des Erlaubnissignals gibt die Dienstleistung der Dienstleistungseinrichtung 36 frei, z.B. Türöffnung, Geldausgabe, Warenbezug, Registrierung usw.

Eine andere Ausführung des Verifikators 22 weist als Aufnahmemittel 32 ein Transportsystem für blatt- oder kartenförmige Dokumente 1 auf. Mit dem Rechengerät 33 ist das vom Rechengerät 33 gesteuerte Aufnahmemittel 32 und zusätzlich zum optischen Leser 26 wenigstens eine Leseinheit 29 zum Übermitteln von Informationen verbunden. Die Leseinheit 29 liest einen oder mehrere Parameter der kryptographischen Operation maschinell aus. Eine Tastatur 28 erübrigt sich für diese Ausführung. Eine Leseinheit 29 ist dann ausreichend, wenn die Parameter der kryptographischen Operation und die Kontrollnummer 9 auf dem Echtheitszertifikat 23 in der gleichen Aufzeichnungstechnik ausgeführt sind.

Für ein System 20, bei dem der Inhaber - PIN verwendet wird, ist die Tastatur 28 für den Inhaber vorgesehen, der sich mit der Inhaber - PIN gegenüber dem Verifikator 22 identifiziert. Die über die Tastatur eingegebene Inhaber - PIN wird in der kryptographischen Operation als Parameter zur Überprüfung der Kontrollnummer 9 verwendet.

Wie beim Validiergerät 21 ist auch eine Identifizierung des Kontrolleurs mittels seiner Benutzer - PIN von Vorteil, um die Hürde für potentielle Einbrecher in das System 20 möglichst hoch anzusetzen. Die Eingabe der richtigen Benutzer - PIN über die Tastatur 28 ermöglicht dem Rechengerät 33 den Benutzer zu identifizieren und den Validator 22 zum Einsatz freizugeben,

Zur Figur 5 ist noch zu bemerken, dass das System 20 mit Vorteil in ein bidirektionales Telefon- oder Computernetzwerk 37 zum Datenaustausch zwischen den Validiergeräten 21 und den Verifikatoren 22 einerseits und einem Rechner 37 andererseits eingebettet ist. Das Validiergerät 21 ist über den Anschluss 28' mit dem Netzwerk 37 und das Netzwerk 37 über eine Leitung 38 mit dem zentralen Rechner 39 verbunden. Neben dem bereits erwähnten Abruf von Daten aus dem zentralen Rechner 39 für den Kode 11 (Figur 2) ermöglicht das Netzwerk 37 im zentralen Rechner 39 eine Negativliste Dokumentennummern 2 von widerrufenen Echtheitszertifikaten 23 anzulegen. Die über das Netzwerk 37 mit dem zentralen Rechner 39 verbundenen Verifikatoren 22 erhalten über eine Datenleitung 40 die regelmässig nachgeführte Negativliste in das Rechengerät 33 (Figur 7) übertragen. Die Negativliste ist in einem Datenspeicher 41 (Figur 7) des Rechengeräts 33 abgelegt, damit auch beim

Ausfall des Netzwerkes 37 widerrufen Echtheitszertifikate 23 von den Verifikatoren 22 erkannt werden.

PATENTANSPRÜCHE

1. Dokument (1) mit einer wenigstens maschinell lesbaren Dokumentennummer (2) auf dem Substrat (6) und einem Speicherfeld (4) für die Aufnahme einer Kontrollnummer (9) dadurch gekennzeichnet, dass auf dem Substrat (6) eine optische Markierung (3) mit einer maschinell lesbaren Kennung (7) angebracht ist, dass das Speicherfeld (4) zur Aufnahme der wenigstens maschinell lesbaren Kontrollnummer (9) eingerichtet ist und dass die Kontrollnummer (9), die das Ergebnis einer kryptographischen Operation mit wenigstens zwei Parametern, der Dokumentennummer (2) und der Kennung (7), und einem ersten geheimen Schlüssel (10) ist, zur Vervollständigung erst bei der Inverkehrbringung als Echtheitszertifikats (23) im Speicherfeld (4) eingesetzt ist.
2. Dokument (1) nach Anspruch 1, dadurch gekennzeichnet, dass die optische Markierung (3) beugungsoptische Strukturen aufweist und dass wenigstens ein Teil der beugungsoptischen Strukturen die maschinell lesbare Kennung (7) enthält.
3. Dokument (1) nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass das Substrat (6) ein Kontrollfeld (5) für die Aufnahme eines wenigstens visuell lesbaren, individuellen und auf eine Person bezogenen Kodes (11) aufweist.
4. Dokument nach Anspruch 1, 2 oder 3, dadurch gekennzeichnet, dass das Speicherfeld (4) auf dem Substrat (6) angeordnet ist und dass nach der Aktivierung die Kontrollnummer (9) im Speicherfeld (4) in wenigstens maschinell lesbaren Zeichen enthalten ist.
5. Dokument (1) nach Anspruch 1, 2, 3 oder 4, dadurch gekennzeichnet, dass im Substrat (6) ein Mikrochip (13) eingelassen ist, dass das Speicherfeld (4) im Speicher (14) des Mikrochips (13) angeordnet ist und dass nach der Aktivierung das Speicherfeld (4) die Kontrollnummer (9) enthält und der einmal eingeschriebene Inhalt des Speicherfelds (4) elektronisch nicht veränderbar ist.
6. Dokument (1) nach Anspruch 1, 2, 3 oder 4, dadurch gekennzeichnet, dass auf dem Substrat (6) ein Magnetstreifen (16) mit dem Speicherfeld (4) angeordnet ist, dass der Magnetstreifen (16) wenigstens das Speicherfeld (4) enthält und dass nach der Aktivierung das Speicherfeld (4) die magnetisch lesbare Kontrollnummer (9) aufweist.
7. Dokument (1) nach Anspruch 1, 2, 3 oder 4, dadurch gekennzeichnet, dass auf dem Substrat (6) ein optischer Informationsträger (17, 17') angeordnet ist, dass der optische Informationsträger (17, 17') wenigstens das Speicherfeld (4) enthält und dass nach der Aktivierung der nicht mehr veränderbare optische Informationsträger (17, 17'') im Speicherfeld (4) die Kontrollnummer (9) in optisch lesbaren Zeichen aufweist.
8. Dokument (1) nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass ein Teil des optischen Informationsträgers (17, 17') die optische Markierung (3) bildet und die Kennung (7) enthält.

9. System (20) bestehend aus wenigstens einem Dokument (1) nach einem der Ansprüche 1 bis 8, einem Validiergerät (21) und einem Verifikator (22), dadurch gekennzeichnet, dass das Dokument (1) wenigstens eine maschinell lesbare Dokumentennummer (2), eine optische Markierung (3) mit einer maschinell lesbare Kennung (7) und ein wenigstens maschinell lesbares Speicherfeld (4) für die Aufnahme einer Kontrollnummer (9) aufweist,
- dass im Validiergerät (21) eine Aufnahmeevorrichtung (25) zur Aufnahme des Dokuments (1) und einen optischen Leser (26) zum maschinellen Ablesen von wenigstens der Kennung (7) angeordnet sind, dass im Validiergerät (21) eine Recheneinheit (24) für kryptographische Operationen mit einem ersten geheimen Schlüssel (10) zum Erzeugen der Kontrollnummer (9) durch Verschlüsseln von wenigstens zwei Parametern, der Dokumentennummer (2) und der Kennung (7), vorhanden ist, dass ein Aufzeichnungsmittel (27) zum Einschreiben der Kontrollnummer (9) in das wenigstens maschinell lesbare Speicherfeld (4) eingerichtet ist,
- dass der Verifikator (22) wenigstens ein Rechengerät (33), einen optischen Leser (26) zum maschinellen Ablesen der Kennung (7) und ein Aufnahmemittel (32) zum Ausrichten eines Echtheitszertifikats (23) zum maschinellen Ablesen aufweist, dass der Verifikator (22) das wenigstens mit Eingabe- und Ablesemitteln (26; 28; 29) verbundene Rechengerät (33) für kryptographische Operationen mit einem zweiten Schlüssel (34) enthält und dass das Rechengerät (33) zur Überprüfung der Zusammengehörigkeit wenigstens der Kontrollnummer (9) und den zum Verschlüsseln benutzten Parametern der kryptographischen Operation, die auf dem Echtheitszertifikat (23) enthalten sind, und zur Darstellung des Vergleichsergebnisses auf einer Anzeige (31) des Verifikators (22) und/oder zur Erzeugung eines Erlaubnissignals eingerichtet ist.
10. System (20) nach Anspruch 9, dadurch gekennzeichnet, dass der Verifikator (22) eine Tastatur (28) für eine manuelle Eingabe einer persönlichen Identifikationsnummer (PIN) zur Freigabe des Verifikators (22) aufweist und dass der Verifikator (22) zum Überprüfen der persönlichen Identifikationsnummer eingerichtet ist.
11. System (20) nach Anspruch 9 oder 10, dadurch gekennzeichnet, dass der Verifikator (22) eine mit dem Rechengerät (33) verbundene Tastatur (28) für eine manuelle Eingabe wenigstens der Dokumentennummer (2) und der Kontrollnummer (9) an das Rechengerät (33) aufweist.
12. System (20) nach einem der Ansprüche 9 bis 11, dadurch gekennzeichnet, dass der Verifikator (22) wenigstens eine mit dem Rechengerät (33) verbundene Leseinheit (29) für eine maschinelle Eingabe der Dokumentennummer (2) und der Kontrollnummer (9) an das Rechengerät (33) aufweist.

13. System (20) nach Anspruch 9, dadurch gekennzeichnet, dass das Validiergerät (21) eine mit der Recheneinheit (24) verbundene Tastatur (28) für eine manuelle Eingabe wenigstens der Dokumentennummer (2) an die Recheneinheit (24) aufweist.
14. System (20) nach Anspruch 9 oder 13, dadurch gekennzeichnet, dass das Validiergerät (21) eine mit der Recheneinheit (24) verbundene Leseinheit (29) für eine maschinelle Eingabe der Dokumentennummer (2) an die Recheneinheit (24) aufweist.
15. System (20) nach Anspruch 9, 13 oder 14, dadurch gekennzeichnet, dass das Validiergerät (21) für die Eingabe eines individuellen, auf eine Person bezogenen Kodes (11) mittels der Tastatur (28) eingerichtet ist und, dass das Aufzeichnungsmittel (27) im Validiergerät (21) zum Einschreiben des Kodes (11) in das Kontrollfeld (5) angeordnet ist.
16. System (20) nach einem der Ansprüche 9 bis 15, dadurch gekennzeichnet, dass die Recheneinheit (24) im Validiergerät (21) derart ausgebildet ist, dass bei der Verschlüsselung der Kontrollnummer (9) eine über eine Tastatur (28) eingegebene persönlichen Identifikationsnummer Nummer der berechtigten Person als Parameter für die Erzeugung der Kontrollnummer (9) einbezogen ist und dass der Verifikator (22) das Erlaubnissignal nur dann im Rechengerät (33) erzeugt, wenn bei der Echtheitsprüfung die persönlichen Identifikationsnummer Nummer über die Tastatur (28) des Verifikators (22) dem Rechengerät (33) als Parameter der kryptographischen Operation einbezogen ist.
17. System (20) nach einem der Ansprüche 9 bis 16, dadurch gekennzeichnet, dass wenigstens ein Validiergerät (21) und wenigstens ein Verifikator (22) über ein Netzwerk (28', 38, 40; 37) mit einem zentralen Rechner (39) zum bidirektionalen Datenaustausch verbunden sind.
18. System (20) nach einem der Ansprüche 9 bis 17, dadurch gekennzeichnet, dass das wenigstens ein Verifikator (22) über eine Signalleitung (35) mit einer Dienstleistungseinrichtung (36) verbunden ist und dass die Dienstleistungseinrichtung (36) zum Freigeben einer Dienstleistung mittels des über die Signalleitung (35) an die Dienstleistungseinrichtung (36) gesandten Erlaubnissignals eingerichtet ist.

ZUSAMMENFASSUNG

Ein Dokument (1) weist auf dem Substrat (6) wenigstens eine Dokumentennummer (2), eine optische Markierung (3) mit einer maschinell lesbaren Kennung (7) und ein Speicherfeld (4) für die Aufnahme einer Kontrollnummer (9) auf. Die Kontrollnummer (9) wird erst im Moment der Abgabe an eine berechnigte Person mittels einer kryptographischen Operation aus wenigstens der Dokumentennummer (2), der Kennung (7) und einem ersten geheimen Schlüssel (10) erzeugt und in das Speicherfeld (4) eingeschrieben. Ein derart erzeugtes Echtheitszertifikat ist mit einem Verifikator unter Verwendung einer kryptographischen Operation und der auf dem Dokument (1) gespeicherten Information mittels eines zweiten Schlüssels auf seine Echtheit überprüfbar.

(Fig. 2)

Fig. 5:

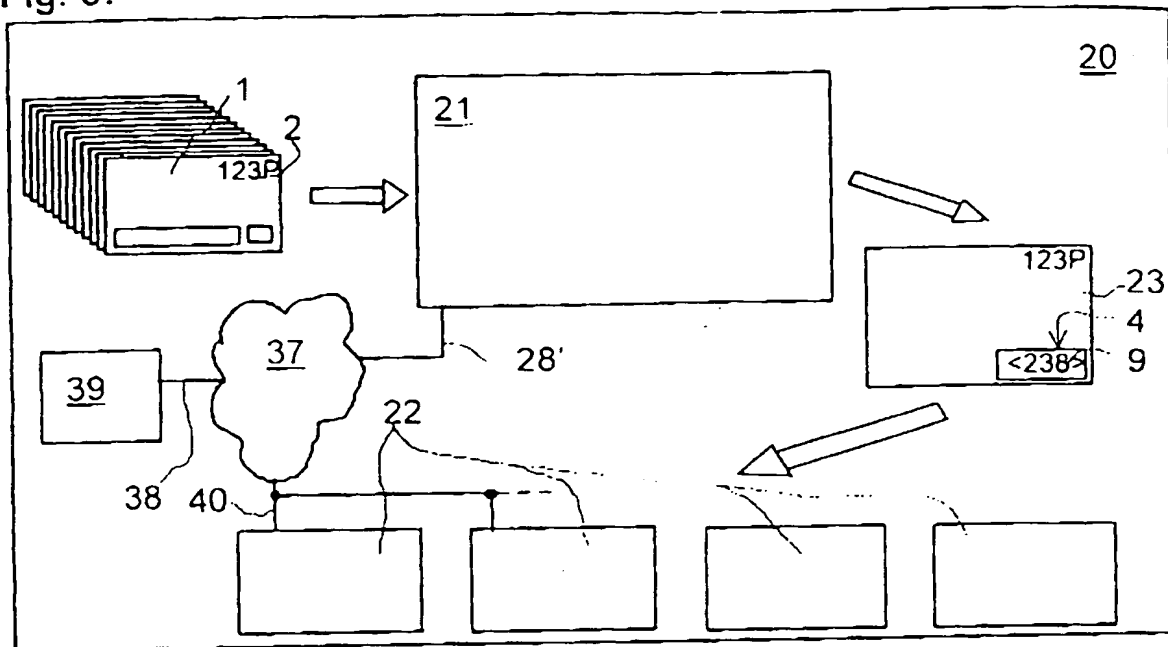


Fig. 6:

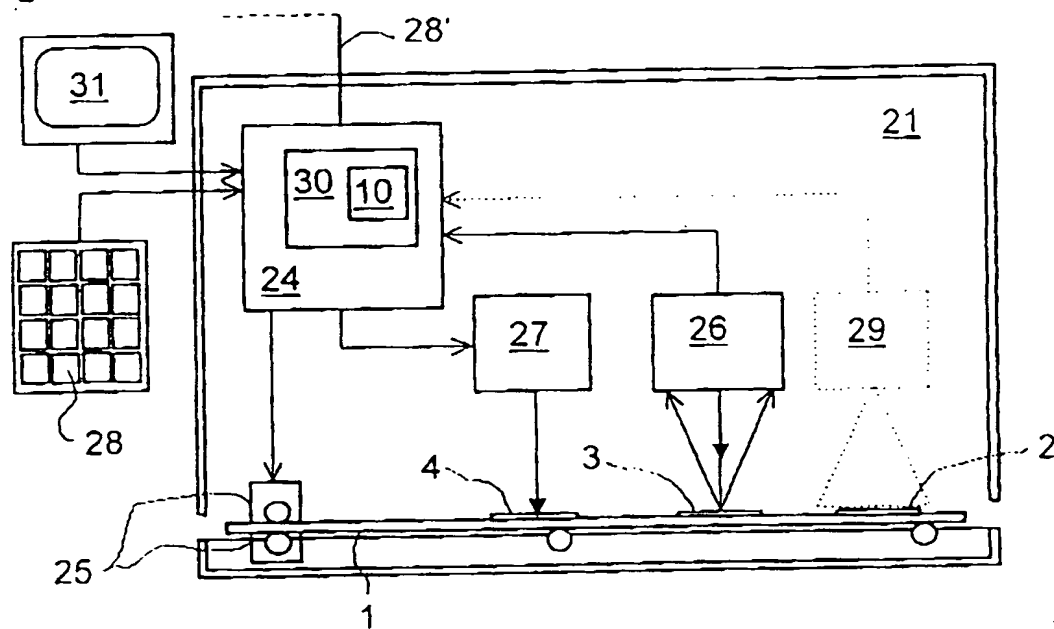
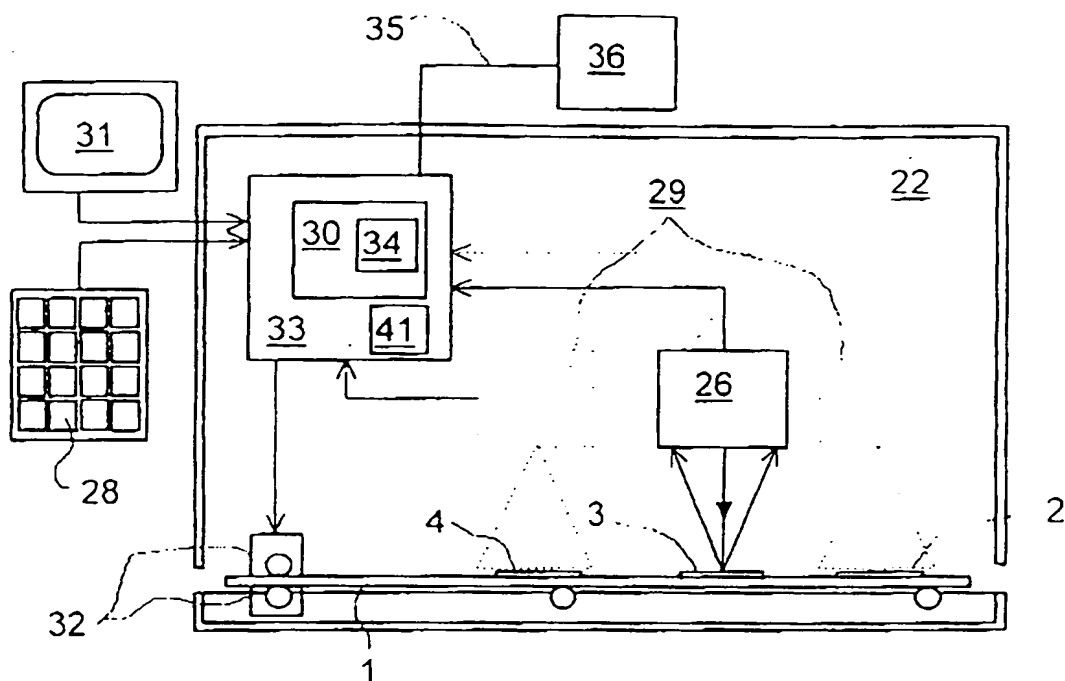


Fig. 7:



VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

Absender: MIT DER INTERNATIONALEN VORLÄUFIGEN
PRÜFUNG BEAUFTRAGTE BEHÖRDE

PCT

SCHRIFTLICHER BESCHIED (Regel 66 PCT)

An:

PÖHLAU, Claus
Louis, Pöhlau, Lohrentz & Segeth
Postfach 30 55
D-90014 Nürnberg
ALLEMAGNE

Louis, Pöhlau & Partner

21. SEP. 2000

Absendedatum
(Tag/Monat/Jahr) 20.09.2000

ANTWORT FÄLLIG innerhalb von **3 Monat(en)**
ab obigem Absendedatum

Aktenzeichen des Anmelders oder Anwalts

T 2900WO/hs

Internationales Aktenzeichen
PCT/EP99/10141

Internationales Anmeldedatum (Tag/Monat/Jahr)
20/12/1999

Prioritätsdatum (Tag/Monat/Jahr)
24/12/1998

Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK

B42D15/10

Anmelder

OVD KINEGRAM AG et al

- Dieser Bescheid ist der **erste** schriftliche Bescheid der mit der internationalen vorläufigen Prüfung beauftragte Behörde
- Dieser Bescheid enthält Angaben zu folgenden Punkten:
 - ☒ Grundlage des Bescheides
 - ☐ Priorität
 - ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
 - ☐ Mangelnde Einheitlichkeit der Erfindung
 - ☒ Begründete Feststellung nach Regel 66.2(a)(ii) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
 - ☐ Bestimmte angeführte Unterlagen
 - ☐ Bestimmte Mängel der internationalen Anmeldung
 - ☒ Bestimmte Bemerkungen zur internationalen Anmeldung
- Der Anmelder wird **aufgefordert**, zu diesem Bescheid **Stellung zu nehmen**

Wann? Siehe oben genannte Frist. Der Anmelder kann vor Ablauf dieser Frist bei der Behörde eine Verlängerung beantragen, siehe Regel 66.2 d).

Wie? Durch Einreichung einer schriftlichen Stellungnahme und gegebenenfalls von Änderungen nach Regel 66.3. Zu Form und Sprache der Änderungen, siehe Regeln 66.8 und 66.9.

Dazu: Hinsichtlich einer zusätzlichen Möglichkeit zur Einreichung von Änderungen, siehe Regel 66.4. Hinsichtlich der Verpflichtung des Prüfers, Änderungen und/oder Gegenvorstellungen zu berücksichtigen, siehe Regel 66.4 bis. Hinsichtlich einer formlosen Erörterung mit dem Prüfer, siehe Regel 66.6.

Wird keine Stellungnahme eingereicht, so wird der internationale vorläufige Prüfungsbericht auf der Grundlage dieses Bescheides erstellt.
- Der Tag, an dem der internationale vorläufige Prüfungsbericht gemäß Regel 69.2 spätestens erstellt sein muß, ist der: 24/04/2001.

Name und Postanschrift der mit der internationalen Prüfung beauftragte Behörde:



Europäisches Patentamt
D-80298 München
Tel. +49 89 2399 - 0 Tx: 523656 epmu d
Fax: +49 89 2399 - 4465

Bevollmächtigter Bediensteter / Prüfer

Schreiber, M

Formalsachbearbeiter (einschl. Fristverlängerung)

Sloan, M
Tel. +49 89 2399 2606



I. Grundlage des Bescheids

1. Dieser Bescheid wurde erstellt auf der Grundlage (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Bescheids als "ursprünglich eingereicht".*):

Beschreibung, Seiten:

1-10 ursprüngliche Fassung

Patentansprüche, Nr.:

1-18 ursprüngliche Fassung

Zeichnungen, Blätter:

1/3-3/3 ursprüngliche Fassung

2. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

- ☐ Beschreibung, Seiten:
- ☐ Ansprüche, Nr.:
- ☐ Zeichnungen, Blatt:

3. Dieser Bescheid ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)):

4. Etwaige zusätzliche Bemerkungen:

V. Begründete Feststellung nach Regel 66.2(a)(ii) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung**1. Feststellung**

Neuheit (N)	Ansprüche	1,3,4
Erfinderische Tätigkeit (IS)	Ansprüche	2,5-8
Gewerbliche Anwendbarkeit (IA)	Ansprüche	

2. Unterlagen und Erklärungen:

siehe Beiblatt

VIII. Bestimmte Bemerkungen zur internationalen Anmeldung

Zur Klarheit der Patentansprüche, der Beschreibung und der Zeichnungen oder zu der Frage, ob die Ansprüche in vollem Umfang durch die Beschreibung gestützt werden, ist folgendes zu bemerken:

siehe Beiblatt

Zu Punkt V

Begründete Feststellung nach Regel 66.2(a)(ii) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

Dokument US-A-3 833 795 (= Dokument D1), das als nächstliegender Stand der Technik angesehen wird, offenbart (vgl. die Zusammenfassung, Spalte 2, Zeile 17 - Spalte 4, Zeile 35) ein Dokument (10) mit einer wenigstens maschinell lesbaren Dokumentennummer (12) auf dem Substrat und einem Speicherfeld für die Aufnahme einer Kontrollnummer (das Dokument gemäß D1 kann ein Scheck oder eine Banknote sein (Spalte 2, Zeile 19) und weist daher zwangsläufig ein Feld (= eine beliebige Gegend auf dem Dokument) auf, das bedruckbar ist und somit als Speicherfeld für die Aufnahme einer Kontrollnummer betrachtet werden kann), wobei auf dem Substrat eine optische Markierung (13) mit einer maschinell lesbaren Kennung (13) angebracht ist, und das Speicherfeld zur Aufnahme der maschinell lesbaren Kontrollnummer eingerichtet ist (jede Gegend auf einem Scheck oder einer Banknote ist zur Aufnahme einer maschinell lesbaren Kontrollnummer eingerichtet).

Der Gegenstand des Anspruchs 1 unterscheidet sich von diesem Stand der Technik nicht (siehe auch Punkt VIII).

Der Gegenstand des Anspruchs ist somit nicht neu (Artikel 33 (2) PCT).

Die abhängigen Ansprüche 2 - 8 enthalten keine Merkmale, die in Kombination mit den Merkmalen irgendeines Anspruchs, auf den sie sich beziehen, die Erfordernisse des PCT in Bezug auf Neuheit bzw. erfinderische Tätigkeit erfüllen. Die Gründe dafür sind die folgenden:

Bei dem zusätzlichen Merkmal des Anspruchs 2 handelt es sich nur um eine von mehreren naheliegenden Möglichkeiten, aus denen der Fachmann ohne erfinderisches Zutun den Umständen entsprechend auswählen würde.

Ein Scheck gemäß Dokument D1 weist zwangsläufig auch die zusätzlichen Merkmale der Ansprüche 3 und 4 auf.

Bei den zusätzlichen Merkmalen der Ansprüche 5 - 8 handelt es sich nur um eine von mehreren naheliegenden Möglichkeiten, aus denen der Fachmann ohne erfinderisches

Zutun den Umständen entsprechend auswählen würde, um Daten in einem Wertdokument zu speichern.

Zu Punkt VIII

Bestimmte Bemerkungen zur internationalen Anmeldung

Das Merkmal in dem Vorrichtungsanspruch 1, dass
- die Kontrollnummer, die das Ergebnis einer kryptographischen Operation mit wenigstens zwei Parametern, der Dokumentennummer und der Kennung, und einem ersten geheimen Schlüssel ist, zur Vervollständigung erst bei der Inverkehrbringung als Echtheitszertifikats im Speicherfeld eingesetzt ist,
bezieht sich auf ein Verfahren zur Verwendung der Vorrichtung und nicht auf die Definition der Vorrichtung anhand ihrer technischen Merkmale. Die beabsichtigten Einschränkungen gehen daher im Widerspruch zu den Erfordernissen des Artikels 6 PCT nicht klar aus dem Anspruch hervor. Das obige Merkmal wird daher für die Beurteilung der Neuheit und erfinderischen Tätigkeit (siehe obigen Punkt V) nicht in Betracht gezogen.

Anspruch 8 sollte sich nur auf Anspruch 7 rückbeziehen, da erst in Anspruch 7 der optische Informationsträger erwähnt wird.

Anspruch 9 ist unklar, denn obwohl das System laut Anspruch 9 ein Dokument nach einem der Ansprüche 1 bis 8 enthält, werden einige der Merkmale eines solchen Dokuments noch einmal aufgeführt.

Außerdem enthält das System laut Anspruch 1 ein Aufnahmemittel zum Ausrichten eines Echtheitszertifikats. Das Echtheitszertifikat ist jedoch nichts anderes als das Dokument (nach Einschreiben der Kontrollnummer) (siehe Seite 6, Zeile 34), was aus dem derzeitigen Anspruchstext nicht klar wird.

PCT

ANTRAG

Der Unterzeichnete beantragt, daß die vorliegende internationale Anmeldung nach dem Vertrag über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens behandelt wird.

Vom Amt auszufüllen

Internationales Aktenzeichen

Internationales Anmeldedatum

Name des Anmeldeamts und "PCT International Application"

Aktenzeichen des Anmelders oder Anwalts (falls gewünscht)
(max. 12 Zeichen) P2900WO

Feld Nr. I BEZEICHNUNG DER ERFINDUNG

Aktivierbares Dokument und System für aktiviertbare Dokumente

Feld Nr. II ANMELDER

Name und Anschrift: (Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)

OVD Kinegram AG
Gubelstrasse 22
CH-6301 Zug
Schweiz

☐ Diese Person ist gleichzeitig Erfinder

Telefonnr.:

041 / 724 2023

Telefaxnr.:

041 / 724 3956

Fernschreibnr.:

Staatsangehörigkeit (Staat):

CH

Sitz oder Wohnsitz (Staat):

CH

☒ Diese Person ist Anmelder für folgende Staaten:

☐

alle Bestimmungsstaaten

☒ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika

☐ nur die Vereinigten Staaten von Amerika

☐ die im Zusatzfeld angegebenen Staaten

Feld Nr. III WEITERE ANMELDER UND/ODER (WEITERE) ERFINDER

Name und Anschrift: (Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)

TOMPKIN Wayne Robert
Oesterliwaldweg 2
CH-5400 Baden
Schweiz

Diese Person ist:

☐ nur Anmelder

☒ Anmelder und Erfinder

☐ nur Erfinder (Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)

Staatsangehörigkeit (Staat):

USA/CH

Sitz oder Wohnsitz (Staat):

CH

☐ Diese Person ist Anmelder für folgende Staaten:

☐

alle Bestimmungsstaaten

☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika

☒ nur die Vereinigten Staaten von Amerika

☐ die im Zusatzfeld angegebenen Staaten

☐ Weitere Anmelder und/oder (weitere) Erfinder sind auf einem Fortsetzungsblatt angegeben.

Feld Nr. IV ANWALT ODER GEMEINSAMER VERTRETER: ODER ZUSTELLANSCHRIFT

Die folgende Person wird hiermit bestellt/ist bestellt worden, um für den (die) Anmelder vor den zuständigen internationalen Behörden in folgender Eigenschaft zu handeln als:

☐

Anwalt

☐

gemeinsamer Vertreter

Name und Anschrift: (Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben.)

Electrowatt Technology Innovation AG
Corporate Intellectual Property Rights
Int. 4470
CH-6301 Zug
Schweiz

Telefonnr.:

041 / 724 2023

Telefaxnr.:

041 / 724 3956

Fernschreibnr.:

☐ Zustellanschrift: Dieses Kästchen ist anzukreuzen, wenn kein Anwalt oder gemeinsamer Vertreter bestellt ist und stattdessen im obigen Feld eine spezielle Zustellanschrift angegeben ist.

Fortsetzung von Feld Nr. III WEITERE ANMELDER UND/ODER (WEITERE) ERFINDER

Wird keines der folgenden Felder benutzt, so sollte dieses Blatt dem Antrag nicht beigelegt werden.

Name und Anschrift: (Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)

STAUB René
Schmiedstrasse 6
CH-6330 Cham
Schweiz

Diese Person ist:

☐ nur Anmelder

☒ Anmelder und Erfinder

☐ nur Erfinder (Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)

Staatsangehörigkeit (Staat):

CH

Sitz oder Wohnsitz (Staat):

CH

Diese Person ist Anmelder für folgende Staaten:

☐ alle Bestimmungsstaaten

☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika

☒ nur die Vereinigten Staaten von Amerika

☐ die im Zusatzfeld angegebenen Staaten

Name und Anschrift: (Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)

Diese Person ist:

☐ nur Anmelder

☐ Anmelder und Erfinder

☐ nur Erfinder (Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)

Staatsangehörigkeit (Staat):

Sitz oder Wohnsitz (Staat):

Diese Person ist Anmelder für folgende Staaten:

☐ alle Bestimmungsstaaten

☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika

☐ nur die Vereinigten Staaten von Amerika

☐ die im Zusatzfeld angegebenen Staaten

Name und Anschrift: (Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)

Diese Person ist:

☐ nur Anmelder

☐ Anmelder und Erfinder

☐ nur Erfinder (Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)

Staatsangehörigkeit (Staat):

Sitz oder Wohnsitz (Staat):

Diese Person ist Anmelder für folgende Staaten:

☐ alle Bestimmungsstaaten

☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika

☐ nur die Vereinigten Staaten von Amerika

☐ die im Zusatzfeld angegebenen Staaten

Name und Anschrift: (Familienname, Vorname; bei juristischen Personen vollständige amtliche Bezeichnung. Bei der Anschrift sind die Postleitzahl und der Name des Staats anzugeben. Der in diesem Feld in der Anschrift angegebene Staat ist der Staat des Sitzes oder Wohnsitzes des Anmelders, sofern nachstehend kein Staat des Sitzes oder Wohnsitzes angegeben ist.)

Diese Person ist:

☐ nur Anmelder

☐ Anmelder und Erfinder

☐ nur Erfinder (Wird dieses Kästchen angekreuzt, so sind die nachstehenden Angaben nicht nötig.)

Staatsangehörigkeit (Staat):

Sitz oder Wohnsitz (Staat):

Diese Person ist Anmelder für folgende Staaten:

☐ alle Bestimmungsstaaten

☐ alle Bestimmungsstaaten mit Ausnahme der Vereinigten Staaten von Amerika

☐ nur die Vereinigten Staaten von Amerika

☐ die im Zusatzfeld angegebenen Staaten

☐ Weitere Anmelder und/oder (weitere) Erfinder sind auf einem zusätzlichen Fortsetzungsblatt angegeben.

Feld Nr. V BESTIMMUNG VON STAATEN

Die folgenden Bestimmungen nach Regel 4.9 Absatz a werden hiermit vorgenommen (bitte die entsprechenden Kästchen ankreuzen: wenigstens ein Kästchen muß angekreuzt werden):

Regionales Patent

- ☒ **AP ARIPO-Patent:** GH Ghana, GM Gambia, KE Kenia, LS Lesotho, MW Malawi, SD Sudan, SL Sierra Leone, SZ Swasiland, UG Uganda, ZW Simbabwe und jeder weitere Staat, der Vertragsstaat des Harare-Protokolls und des PCT ist
- ☒ **EA Eurasisches Patent:** AM Armenien, AZ Aserbaidshan, BY Belarus, KG Kirgisistan, KZ Kasachstan, MD Republik Moldau, RU Russische Föderation, TJ Tadschikistan, TM Turkmenistan und jeder weitere Staat, der Vertragsstaat des Eurasischen Patentübereinkommens und des PCT ist
- ☒ **EP Europäisches Patent:** AT Österreich, BE Belgien, CH und LI Schweiz und Liechtenstein, CY Zypern, DE Deutschland, DK Dänemark, ES Spanien, FI Finnland, FR Frankreich, GB Vereinigtes Königreich, GR Griechenland, IE Irland, IT Italien, LU Luxemburg, MC Monaco, NL Niederlande, PT Portugal, SE Schweden und jeder weitere Staat, der Vertragsstaat des Europäischen Patentübereinkommens und des PCT ist
- ☒ **OA OAPI-Patent:** BF Burkina Faso, BJ Benin, CF Zentralafrikanische Republik, CG Kongo, CI Côte d'Ivoire, CM Kamerun, GA Gabun, GN Guinea, GW Guinea-Bissau, ML Mali, MR Mauretanien, NE Niger, SN Senegal, TD Tschad, TG Togo und jeder weitere Staat, der Vertragsstaat der OAPI und des PCT ist (falls eine andere Schutzrechtsart oder ein sonstiges Verfahren gewünscht wird, bitte auf der gepunkteten Linie angeben)

Nationales Patent (falls eine andere Schutzrechtsart oder ein sonstiges Verfahren gewünscht wird, bitte auf der gepunkteten Linie angeben):

- | | |
|---|--|
| <input checked="" type="checkbox"/> AE Vereinigte Arabische Emirate | <input checked="" type="checkbox"/> LR Liberia |
| <input checked="" type="checkbox"/> AL Albanien | <input checked="" type="checkbox"/> LS Lesotho |
| <input checked="" type="checkbox"/> AM Armenien | <input checked="" type="checkbox"/> LT Litauen |
| <input checked="" type="checkbox"/> AT Österreich | <input checked="" type="checkbox"/> LU Luxemburg |
| <input checked="" type="checkbox"/> AU Australien | <input checked="" type="checkbox"/> LV Lettland |
| <input checked="" type="checkbox"/> AZ Aserbaidshan | <input checked="" type="checkbox"/> MD Republik Moldau |
| <input checked="" type="checkbox"/> BA Bosnien-Herzegowina | <input checked="" type="checkbox"/> MG Madagaskar |
| <input checked="" type="checkbox"/> BB Barbados | <input checked="" type="checkbox"/> MK Die ehemalige jugoslawische Republik Mazedonien |
| <input checked="" type="checkbox"/> BG Bulgarien | <input checked="" type="checkbox"/> MN Mongolei |
| <input checked="" type="checkbox"/> BR Brasilien | <input checked="" type="checkbox"/> MW Malawi |
| <input checked="" type="checkbox"/> BY Belarus | <input checked="" type="checkbox"/> MX Mexiko |
| <input checked="" type="checkbox"/> CA Kanada | <input checked="" type="checkbox"/> NO Norwegen |
| <input checked="" type="checkbox"/> CH und LI Schweiz und Liechtenstein | <input checked="" type="checkbox"/> NZ Neuseeland |
| <input checked="" type="checkbox"/> CN China | <input checked="" type="checkbox"/> PL Polen |
| <input checked="" type="checkbox"/> CU Kuba | <input checked="" type="checkbox"/> PT Portugal |
| <input checked="" type="checkbox"/> CZ Tschechische Republik | <input checked="" type="checkbox"/> RO Rumänien |
| <input checked="" type="checkbox"/> DE Deutschland | <input checked="" type="checkbox"/> RU Russische Föderation |
| <input checked="" type="checkbox"/> DK Dänemark | <input checked="" type="checkbox"/> SD Sudan |
| <input checked="" type="checkbox"/> EE Estland | <input checked="" type="checkbox"/> SE Schweden |
| <input checked="" type="checkbox"/> ES Spanien | <input checked="" type="checkbox"/> SG Singapur |
| <input checked="" type="checkbox"/> FI Finnland | <input checked="" type="checkbox"/> SI Slowenien |
| <input checked="" type="checkbox"/> GB Vereinigtes Königreich | <input checked="" type="checkbox"/> SK Slowakei |
| <input checked="" type="checkbox"/> GD Grenada | <input checked="" type="checkbox"/> SL Sierra Leone |
| <input checked="" type="checkbox"/> GE Georgien | <input checked="" type="checkbox"/> TJ Tadschikistan |
| <input checked="" type="checkbox"/> GH Ghana | <input checked="" type="checkbox"/> TM Turkmenistan |
| <input checked="" type="checkbox"/> GM Gambia | <input checked="" type="checkbox"/> TR Türkei |
| <input checked="" type="checkbox"/> HR Kroatien | <input checked="" type="checkbox"/> TT Trinidad und Tobago |
| <input checked="" type="checkbox"/> HU Ungarn | <input checked="" type="checkbox"/> UA Ukraine |
| <input checked="" type="checkbox"/> ID Indonesien | <input checked="" type="checkbox"/> UG Uganda |
| <input checked="" type="checkbox"/> IL Israel | <input checked="" type="checkbox"/> US Vereinigte Staaten von Amerika |
| <input checked="" type="checkbox"/> IN Indien | <input checked="" type="checkbox"/> UZ Usbekistan |
| <input checked="" type="checkbox"/> IS Island | <input checked="" type="checkbox"/> VN Vietnam |
| <input checked="" type="checkbox"/> JP Japan | <input checked="" type="checkbox"/> YU Jugoslawien |
| <input checked="" type="checkbox"/> KE Kenia | <input checked="" type="checkbox"/> ZA Südafrika |
| <input checked="" type="checkbox"/> KG Kirgisistan | <input checked="" type="checkbox"/> ZW Simbabwe |
| <input checked="" type="checkbox"/> KP Demokratische Volksrepublik Korea | |
| <input checked="" type="checkbox"/> KR Republik Korea | Kästchen für die Bestimmung von Staaten, die dem PCT nach der Veröffentlichung dieses Formblatts beigetreten sind: |
| <input checked="" type="checkbox"/> KZ Kasachstan | <input type="checkbox"/> |
| <input checked="" type="checkbox"/> LC Saint Lucia | <input type="checkbox"/> |
| <input checked="" type="checkbox"/> LK Sri Lanka | <input type="checkbox"/> |

Erklärung bzgl. vorsorglicher Bestimmungen: Zusätzlich zu den oben genannten Bestimmungen nimmt der Anmelder nach Regel 4.9 Absatz b auch alle anderen nach dem PCT zulässigen Bestimmungen vor mit Ausnahme der im Zusatzfeld genannten Bestimmungen, die von dieser Erklärung ausgenommen sind. Der Anmelder erklärt, daß diese zusätzlichen Bestimmungen unter dem Vorbehalt einer Bestätigung stehen und jede zusätzliche Bestimmung, die vor Ablauf von 15 Monaten ab dem Prioritätsdatum nicht bestätigt wurde, nach Ablauf dieser Frist als vom Anmelder zurückgenommen gilt. (Die Bestätigung einer Bestimmung erfolgt durch die Einreichung einer Mitteilung, in der diese Bestimmung angegeben wird, und die Zahlung der Bestimmungs- und der Bestätigungsgebühr. Die Bestätigung muß beim Anmeldeamt innerhalb der Frist von 15 Monaten eingehten.)

Feld Nr. VI PRIORITÄTSANSPRUCH		<input type="checkbox"/> Weitere Prioritätsansprüche sind im Zusatzfeld angegeben.		
Anmeldedatum der früheren Anmeldung (Tag/Monat/Jahr)	Anzeichen der früheren Anmeldung	Ist die frühere Anmeldung eine:		
		nationale Anmeldung: Staat	regionale Anmeldung: regionales Amt	internationale Anmeldung: Anmeldeamt
Zeile (1) 24.12.1998	1998 2557/98	Schweiz		
Zeile (2)		246	2001(3C)	
Zeile (3)				

☐ Das Anmeldeamt wird ersucht, eine beglaubigte Abschrift der oben in der (den) Zeile(n) _____ bezeichneten früheren Anmeldung(en) zu erstellen und dem internationalen Büro zu übermitteln (nur falls die frühere Anmeldung(en) bei dem Amt eingereicht worden ist(sind), das für die Zwecke dieser internationalen Anmeldung Anmeldeamt ist)

* Falls es sich bei der früheren Anmeldung um eine ARIPO-Anmeldung handelt, so muß in dem Zusatzfeld mindestens ein Staat angegeben werden, der Mitgliedstaat der Pariser Verbandsübereinkunft zum Schutz des gewerblichen Eigentums ist und für den die frühere Anmeldung eingereicht wurde.

Feld Nr. VII INTERNATIONALE RECHERCHENBEHÖRDE

Wahl der internationalen Recherchenbehörde (ISA)
(falls zwei oder mehr als zwei internationale Recherchen-
behörden für die Ausführung der internationalen Recherche
zuständig sind, geben Sie die von Ihnen gewählte Behörde an;
der Zweibuchstaben-Code kann benutzt werden):

Antrag auf Nutzung der Ergebnisse einer früheren Recherche: Bezugnahme auf diese
frühere Recherche (falls eine frühere Recherche bei der internationalen Recherchenbehörde
beantragt oder von ihr durchgeführt worden ist):

ISA /

Datum (Tag/Monat/Jahr)

Aktenzeichen

Staat (oder regionales Amt)

Feld Nr. VIII KONTROLLISTE; EINREICHUNGSSPRACHE

Diese internationale Anmeldung enthält
die folgende Anzahl von Blättern:

Antrag : 4
Beschreibung (ohne
Sequenzprotokollteil) : 10
Ansprüche : 3
Zusammenfassung : 1
Zeichnungen : 3
Sequenzprotokollteil
der Beschreibung :
Blattzahl insgesamt : 21

Dieser internationalen Anmeldung liegen die nachstehend angekreuzten Unterlagen bei:

1. ☒ Blatt für die Gebührenberechnung
2. ☐ Gesonderte unterzeichnete Vollmacht
3. ☐ Kopie der allgemeinen Vollmacht: Aktenzeichen (falls vorhanden):
4. ☐ Begründung für das Fehlen einer Unterschrift
5. ☒ Prioritätsbeleg(e), in Feld Nr. VI durch
folgende Zeilennummer gekennzeichnet:
6. ☐ Übersetzung der internationalen Anmeldung in die folgende Sprache:
7. ☐ Gesonderte Angaben zu hinterlegten Mikroorganismen oder anderem biologischen Material
8. ☐ Protokoll der Nucleotid- und/oder Aminosäuresequenzen in computerlesbarer Form
9. ☐ Sonstige (einzeln auflisten):

Abbildung der Zeichnungen, die
mit der Zusammenfassung
veröffentlicht werden soll (Nr.):

2

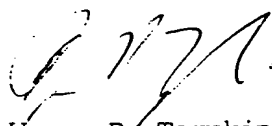
Sprache, in der die
internationale Anmeldung
eingereicht wird:

deutsch

Feld Nr. IX UNTERSCHRIFT DES ANMELDERS ODER DES ANWALTS

Der Name jeder unterzeichnenden Person ist neben der Unterschrift zu wiederholen, und es ist anzugeben, sofern sich dies nicht eindeutig
aus dem Antrag ergibt, in welcher Eigenschaft die Person unterzeichnet.

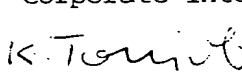
Electrowatt Technology Innovation AG
Corporate Intellectual Property Rights



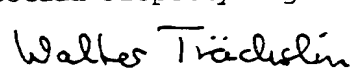
Wayne R. Tompkin



René Staub



Kurt Toniolo



Walter Trächslin

Vom Anmeldeamt auszufüllen

1. Datum des tatsächlichen Eingangs dieser internationalen Anmeldung:	2. Zeichnungen <input type="checkbox"/> einge- gangen: <input type="checkbox"/> nicht ein- gegangen:
3. Geändertes Eingangsdatum aufgrund nachträglich, jedoch fristgerecht eingegangener Unterlagen oder Zeichnungen zur Vervollständigung dieser internationalen Anmeldung:	
4. Datum des fristgerechten Eingangs der angeforderten Richtigstellungen nach Artikel 11(2) PCT:	
5. Internationale Recherchenbehörde (falls zwei oder mehr zuständig sind): ISA /	6. <input type="checkbox"/> Übermittlung des Recherchenexemplars bis zur Zahlung der Recherchegebühr aufgeschoben

Vom Internationalen Büro auszufüllen

Datum des Eingangs des Aktenexemplars
beim Internationalen Büro:

LOUIS. PÖHLAU, LOHRENTZ & SEGETH
PATENTANWÄLTE
EUROPEAN PATENT ATTORNEYS

DR. DIETER LOUIS († 1994)
CINUS PÖHLAU, DIPL.-PHYS.
FRANK LOHRENTZ († 1999)
WOLFG. SEGETH, DIPL.-PHYS.

POSTANSCHRIFT/MAILING ADDRESS:
D-90014 NÜRNBERG
POSTFACH 100, BOX 8055
TELEFON (0911) 5105-60
TELEFAX (0911) 5105-42
E-MAIL: office@burgpatent.de
HAUSANSCHRIFT/PREMISES:
D-90409 NÜRNBERG
MERIANSTRASSE 16

PCT Chapter II
MU DG 2

Europäisches Patentamt
Erhardtstraße 27

80331 München

T/2900WO/WO/30-in

Unser Zeichen / Our reference

18. Dezember 2000

Vorab per Telefax

PCT-Anmeldung

Land

Anmelder / Inhaber

Titel

Ihr Zeichen

: PCT/EP99/10141
: International
: OVD Kinegram AG
: Aktivierbares Dokument und System für aktivierbare Dok.
:

Auf den ersten schriftlichen Bescheid gem. Regel 66 PCT vom 20.09.2000:

1.

In der Anlage werden neue Anspruchsseiten 11 bis 13 (gekennzeichnet links unten mit P2900WO/28.11.2000) überreicht mit der Bitte, die beiliegenden neuen Ansprüche der weiteren Prüfung zugrunde zu legen.

Im neuen Anspruch 1 wird versucht, den Beanstandungen unter Punkt VIII des Bescheids zu entsprechen. Insbesondere wurde Anspruch 1 derart umformuliert, daß sich nunmehr klar ergibt, daß das in dem schriftlichen Bescheid erwähnte Teilmerkmal, welches als Verfahrensmerkmal angesehen wurde, tatsächlich kein Verfahrensmerkmal darstellt. Ausweislich des neuen Anspruchs 1 ist nun maßgeblich, daß auf dem Substrat neben der Dokumentennummer und dem Speicherfeld für die Kontrollnummer eine optische Markierung mit einer maschinell lesbaren Kennung angebracht ist, wobei weiterhin die Kontrollnummer in ganz bestimmter Weise ausgehend von der Dokumentennummer und der optischen Kennung in einer kryptographischen Operation unter Verwendung eines ersten geheimen Schlüssels erzeugt ist, und wobei weiterhin das Dokument dadurch zu einem Echtheitszertifikat – bei Aktivierung im Rahmen des Inverkehrbringens – umgewandelt wird, indem die entsprechend gebildete Kontrollnummer in das Speicherfeld eingeschrieben ist. Der neue Anspruch 1 beinhaltet somit durchgehend Merkmale, die das erfindungsgemäße Dokument – bzw. nach Aktivierung Echtheitszertifikat – selbst kennzeichnen. Das möglicherweise noch verfahrensmäßige Merkmal, wonach die Information im Speicherfeld erst bei der Inverkehrbringung vervollständigt werden soll, wurde nur deswegen im Anspruch 1 beibehalten, weil andernfalls möglicherweise eine unzulässige Änderung vorläge.

Bezüglich der weiteren Ansprüche ist festzustellen, daß sie im wesentlichen nur redaktionell überarbeitet wurden. Anspruch 9 wurde unter Berücksichtigung der Bemerkungen im Bescheid revidiert, wobei hinsichtlich der in den Ansprüchen vorgenommenen Ergänzungen bzw. Änderungen auf folgende Umstände bzw. Textpassagen der ursprünglichen Beschreibung verwiesen wird:

Anspruch 1: Seite 2, Zeilen 2 bis 3 sowie Seite 5, Zeilen 7 bis 10

Ansprüche 2 bis 4: unverändert

Ansprüche 5 und 6: neue Rückbeziehung auf Ansprüche 1 bis 3

Anspruch 7: unverändert

Anspruch 8: neue Rückbeziehung auf Anspruch 7

Anspruch 9: „Transportvorrichtung“: Seite 5, Zeile 12

„verbundene Recheneinheit“: Seite 5, Zeilen 18 bis 20

„abgelesene Kennung“: Seite 6, Zeile 30

„Vervollständigung des Dokuments“: Seite 5, Zeile 7 bis 10

„zu überprüfendes Echtheitszertifikat“: Seite 8, Zeile 17

Anspruch 10: „des Benutzers“: Seite 9, Zeilen 21 bis 24

Anspruch 11: „Parameter“: Seite 8, Zeile 20 bis 22

Anspruch 12: „Parameter“: Seite 8, Zeile 20 bis 22, neue Rückbeziehung auf Anspruch 9 oder 11

Ansprüche 13 und 14:
neue Rückbeziehung auf Ansprüche 9 bis 12

Anspruch 15: „Code (11) einer der Parameter“: Seite 7, Zeile 28 bis Seite 8, Zeile 3; neue Rückbeziehung auf Ansprüche 9 bis 14

Anspruch 16: „Nummer“: (ein offensichtlicher Fehler) an zwei Stellen hinter „Identifikationsnummer“, gestrichen

Ansprüche 17 und 18:
unverändert

2.
Zu den Ausführungen unter V des Bescheids, wo nach Auffassung des Prüfers Zweifel an der Neuheit bzw. erfinderischen Tätigkeit der Ansprüche 1 bis 8 geäußert werden, erlauben wir uns folgendes festzustellen:

Die Entgegenhaltung US-3,833,795 (= D1) ist als nächstliegender Stand der Technik anzusehen und ist daher schon in der Einleitung in der ursprünglich eingereichten Fassung der Anmeldung berücksichtigt.

Die D1 beschreibt ein Dokument, das mit einer Referenznummer (reference numeral 11) versehen ist. Die oben links gedruckte Referenznummer ist, wie in der Figur 1 der D1 gezeigt, unten rechts auf dem Dokument wiederholt. Die Referenznummer ist aus zwei Zahlengruppen zusammengesetzt, wobei im gezeigten Beispiel als linke Zahlengruppe eine Seriennummer (identification number 12) und als rechte Zahlengruppe eine mehrstellige Zufallszahl als Kontrollzahl (control number 13) eingesetzt ist. Da keine Relation zwischen der Seriennummer und der Kontrollzahl besteht, ist die Referenznummer von jedem in Verkehr gebrachten Dokument in eine Liste einzutragen, damit später die Echtheit des Dokuments anhand der Liste verifiziert werden kann (D1, Spalte 3, Zeile 1 bis 28). Die D1 lehrt also nur, zwei Zahlen zusammenzustellen und in ein Feld einzuschreiben.

Im Gegensatz dazu weist das Dokument der vorliegenden Anmeldung neben der aus der D1 bekannten Seriennummer und Kontrollzahl zusätzlich eine optische Markierung mit einer Kennung auf. Es ist daher wenigstens auch die Kennung abzulesen. Ausserdem ist die Kontrollzahl nicht eine Zufallszahl, die bei Echtheitsprüfung die Verwendung einer Liste der echten Dokumentnummern voraussetzt, sondern sie ist ein kryptographisches Produkt aus der Seriennummer und der Kennung. Die Echtheit des Dokuments kann daher ohne die Liste der echten Dokumentnummern, beispielsweise in einem geeigneten Gerät, mit Hilfe der auf dem Dokument verzeichneten Kontrollzahl verifiziert werden.

Die Neuheit des Anspruchs 1 ist somit durch die D1 nicht vorweggenommen.

Die D1 weist weder eine optische Markierung mit einer maschinell lesbaren Kennung auf noch eine von der Seriennummer und der Kennung abhängige Kontrollzahl. Weiter geht aus der D1 hervor, dass auf dem Dokument selbst nicht alle Informationen vorhanden sind, um die Echtheit des Dokuments maschinell festzustellen. Im Gegenteil wird ausdrücklich darauf hingewiesen, dass die Verifikation des Dokuments auf die Liste der echten Dokumentnummern gestützt ist.


Die Idee, alle für die Überprüfung der Echtheit notwendigen Informationen auf dem Dokument unterzubringen, damit nicht auf Listen zurückgegriffen werden muss, ist D1 nicht zu entnehmen und auch durch D1 nicht nahegelegt und ist daher als Anzeichen des notwendigen erfinderischen Schrittes zu werten.

Zur D1 ist weiter zu bemerken, dass die darin erwähnten Arten von Dokumenten, wie Wertpapiere (Aktienzertifikate, Obligationen usw.), Cheques, Banknoten und ähnliche, gegen Fälschung geschützt werden. Solche Dokumente werden zunächst gedruckt und die Bildwiedergabe geprüft, bevor der Aufdruck der Seriennummer und Kontrollnummer in einem separaten Arbeitsgang erfolgt. Anschliessend werden die fertiggestellten Dokumente geschnitten, abgepackt und in einem Sicherheitsraum geschützt gelagert, bis eine Abgabe ans Publikum erfolgt.

Im Gegensatz dazu ist das Dokument gemäß der Erfindung, das typisch ein Ausweis für ein Individuum ist, bis zur Abgabe an das Individuum, d.h. der sogenannten Aktivierung, nicht vollständig. Erst das Einsetzen der Kontrollzahl im Speicherfeld macht aus dem Dokument ein Echtheitszertifikat.

Aufgrund vorstehender Ausführungen ist somit davon auszugehen, daß die nunmehr vorliegenden Ansprüche 1 bis 18 den Bestimmungen des Artikels 33 PCT entsprechen, weshalb gebeten wird, in einem weiteren Bescheid, eventuell im internationalen Prüfungsbericht, die Neuheit und erfinderische Tätigkeit bezüglich der nunmehr vorliegenden Ansprüche anzuerkennen. Sollte sich die internationale Behörde der vertretenen Auffassung nicht anschließen können, wird darum gebeten, eine weitere Möglichkeit zur Einreichung von Änderungen oder Gegenvorstellungen nach Regel 66.4 PCT einzuräumen.

Es wird in diesem Zusammenhang allerdings darauf hingewiesen, daß nicht beabsichtigt ist, im Rahmen des vorläufigen internationalen Prüfungsverfahrens eine Anpassung bzw. Überarbeitung auch der Beschreibung vorzunehmen, weil dies nur unnötige Übersetzungskosten und möglicherweise Probleme im Prüfungsverfahren in einigen der PCT-Mitgliedsländer verursachen könnte.


Patentanwalt

Anlagen

Neue Seiten 11-13 mit Ansprüchen 1-18

PATENTANSPRÜCHE

1. Dokument (1) mit einer wenigstens maschinell lesbaren Dokumentennummer (2) auf dem Substrat (6) und einem Speicherfeld (4) für die Aufnahme einer wenigstens maschinell lesbaren Kontrollnummer (9), dadurch gekennzeichnet, dass auf dem Substrat (6) eine optische Markierung (3) mit einer maschinell lesbaren Kennung (7) angebracht ist, und dass zur Aktivierung ein Echtheitszertifikat (23) die wenigstens maschinell lesbare Information im Speicherfeld (4) durch Einschreiben der das Ergebnis einer kryptographischen Operation mit wenigstens zwei Parametern, der Dokumentennummer (2) und der Kennung (7), und einem ersten geheimen Schlüssel (10) bildenden Kontrollnummer (9) in das Speicherfeld (4) erst bei der Inverkehrbringung vervollständigt ist.
2. Dokument (1) nach Anspruch 1, dadurch gekennzeichnet, dass die optische Markierung (3) beugungsoptische Strukturen aufweist, und dass wenigstens ein Teil der beugungsoptischen Strukturen die maschinell lesbare Kennung (7) enthält.
3. Dokument (1) nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass das Substrat (6) ein Kontrollfeld (5) für die Aufnahme eines wenigstens visuell lesbaren, individuellen und auf eine Person bezogenen Codes (11) aufweist.
4. Dokument nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass das Speicherfeld (4) auf dem Substrat (6) angeordnet ist und dass nach der Aktivierung die Kontrollnummer (9) im Speicherfeld (4) in wenigstens maschinell lesbaren Zeichen enthalten ist.
5. Dokument (1) nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass im Substrat (6) ein Mikrochip (13) eingelassen ist, dass das Speicherfeld (4) im Speicher (14) des Mikrochips (13) angeordnet ist und dass nach der Aktivierung das Speicherfeld (4) die Kontrollnummer (9) enthält und der einmal eingeschriebene Inhalt des Speicherfelds (4) elektronisch nicht veränderbar ist.
6. Dokument (1) nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass auf dem Substrat (6) ein Magnetstreifen (16) mit dem Speicherfeld (4) angeordnet ist, dass der Magnetstreifen (16) wenigstens das Speicherfeld (4) enthält und dass nach der Aktivierung das Speicherfeld (4) die magnetisch lesbare Kontrollnummer (9) aufweist.
7. Dokument (1) nach Anspruch 1, 2, 3 oder 4, dadurch gekennzeichnet, dass auf dem Substrat (6) ein optischer Informationsträger (17, 17') angeordnet ist, dass der optische Informationsträger (17, 17') wenigstens das Speicherfeld (4) enthält und dass nach der Aktivierung der nicht mehr veränderbare optische Informationsträger (17, 17') im Speicherfeld (4) die Kontrollnummer (9) in optisch lesbaren Zeichen aufweist.
8. Dokument (1) nach Anspruch 7, dadurch gekennzeichnet, dass ein Teil des optischen Informationsträgers (17, 17') die optische Markierung (3) bildet und die Kennung (7) enthält.

9. System (20) bestehend aus wenigstens einem Dokument (1) nach einem der Ansprüche 1 bis 8, einem Validiergerät (21) und einem Verifikator (22),
dadurch gekennzeichnet.

dass im Validiergerät (21) eine Transportvorrichtung (25) zur Aufnahme des Dokuments (1), ein
5 Aufzeichnungsmittel (27) und ein optischer Leser (26) zum maschinellen Ablesen von wenigstens der
Kennung (7) angeordnet sind, dass das Validiergerät (21) weiter eine mit dem Aufzeichnungsmittel
(27) und dem optischen Leser (26) verbundene Recheneinheit (24) für kryptographische Operationen
mit einem ersten geheimen Schlüssel (10) zum Erzeugen der Kontrollnummer (9) durch Verschlüsseln
10 von wenigstens zwei Parametern, der Dokumentennummer (2) und der vom optischen Leser (26)
abgelesene Kennung (7), umfasst, dass das Aufzeichnungsmittel (27) zum Einschreiben der
Kontrollnummer (9) zum Aktivieren des Dokuments (1) zum Echtheitszertifikat (23) in das
wenigstens maschinell lesbare Speicherfeld (4) eingerichtet ist,
dass der Verifikator (22) wenigstens ein Rechenggerät (33), einen optischen Leser (26) zum
15 maschinellen Ablesen der Kennung (7) und ein Aufnahmemittel (32) zum Ausrichten eines zu
überprüfenden Echtheitszertifikats (23) zum maschinellen Ablesen aufweist, dass das Rechenggerät
(33) mit Eingabe- und Ablesemitteln (26; 28; 29) verbunden und für kryptographische Operationen
mit einem zweiten Schlüssel (34) sowie zur Überprüfung der Zusammengehörigkeit wenigstens der
Kontrollnummer (9) und der zum Verschlüsseln benutzten Parametern der kryptographischen
20 Operation, die auf dem Echtheitszertifikat (23) enthalten sind, und zur Darstellung des
Vergleichsergebnisses auf einer Anzeige (31) des Verifikators (22) und/oder zur Erzeugung eines
Erlaubnissignals eingerichtet ist.

10. System (20) nach Anspruch 9, dadurch gekennzeichnet, dass der Verifikator (22) eine
Tastatur (28) für eine manuelle Eingabe einer persönlichen Identifikationsnummer (PIN) zur Freigabe
des Verifikators (22) aufweist und dass der Verifikator (22) zum Überprüfen der persönlichen
25 Identifikationsnummer des Benutzers eingerichtet ist.

11. System (20) nach Anspruch 9 oder 10, dadurch gekennzeichnet, dass der Verifikator (22) eine mit
dem Rechenggerät (33) verbundene Tastatur (28) für eine manuelle Eingabe der Parameter der
kryptographischen Operation an das Rechenggerät (33) aufweist, wobei die Parameter wenigstens die
Dokumentennummer (2) und die Kontrollnummer (9) umfassen.

30 12. System (20) nach einem der Ansprüche 9 oder 11, dadurch gekennzeichnet, dass der
Verifikator (22) wenigstens eine mit dem Rechenggerät (33) verbundene Leseinheit (29) für eine
maschinelle Eingabe der Parameter der kryptographischen Operation an das Rechenggerät (33)
aufweist, wobei die Parameter wenigstens die Dokumentennummer (2) und die Kontrollnummer (9)
umfassen.

13. System (20) nach einem der Ansprüche 9 bis 12, dadurch gekennzeichnet, dass das Validiergerät (21) eine mit der Recheneinheit (24) verbundene Tastatur (28) für eine manuelle Eingabe wenigstens der Dokumentennummer (2) an die Recheneinheit (24) aufweist.

5 14. System (20) nach einem der Ansprüche 9 bis 12, dadurch gekennzeichnet, dass das Validiergerät (21) eine mit der Recheneinheit (24) verbundene Leseinheit (29) für eine maschinelle Eingabe der Dokumentennummer (2) an die Recheneinheit (24) aufweist.

15. System (20) nach einem der Ansprüche 9 bis 14, dadurch gekennzeichnet, dass das Validiergerät (21) für die Eingabe eines individuellen, auf eine berechnete Person bezogenen Codes (11) mittels einer Tastatur (28) eingerichtet ist, dass das Validiergerät (21) ein Aufzeichnungsmittel (27) im
10 Validiergerät (21) zum Einschreiben des Codes (11) in das Kontrollfeld (5) umfasst und dass der Code (11) einer der Parameter für die Erzeugung der Kontrollnummer (9) im Validiergerät (21) bzw. für die Echtheitsprüfung im Verifikator (22) ist.

16. System (20) nach einem der Ansprüche 9 bis 15, dadurch gekennzeichnet, dass die Recheneinheit (24) im Validiergerät (21) derart ausgebildet ist, dass bei der Verschlüsselung der
15 Kontrollnummer (9) eine über eine Tastatur (28) eingegebene persönlichen Identifikationsnummer der berechtigten Person als Parameter für die Erzeugung der Kontrollnummer (9) einbezogen ist und dass der Verifikator (22) das Erlaubnissignal nur dann im Rechengerät (33) erzeugt, wenn bei der Echtheitsprüfung die persönlichen Identifikationsnummer über die Tastatur (28) des Verifikators (22) dem Rechengerät (33) als Parameter der kryptographischen Operation einbezogen ist.

20 17. System (20) nach einem der Ansprüche 9 bis 16, dadurch gekennzeichnet, dass wenigstens ein Validiergerät (21) und wenigstens ein Verifikator (22) über ein Netzwerk (28', 38, 40; 37) mit einem zentralen Rechner (39) zum bidirektionalen Datenaustausch verbunden sind.

18. System (20) nach einem der Ansprüche 9 bis 17, dadurch gekennzeichnet, dass das wenigstens ein Verifikator (22) über eine Signalleitung (35) mit einer Dienstleistungseinrichtung (36) verbunden
25 ist und dass die Dienstleistungseinrichtung (36) zum Freigeben einer Dienstleistung mittels des über die Signalleitung (35) an die Dienstleistungseinrichtung (36) gesandten Erlaubnissignals eingerichtet ist.

PCT
 ORGANISATION FÜR GEISTIGES EIGENTUM
 Internationales Büro
 INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE
 INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

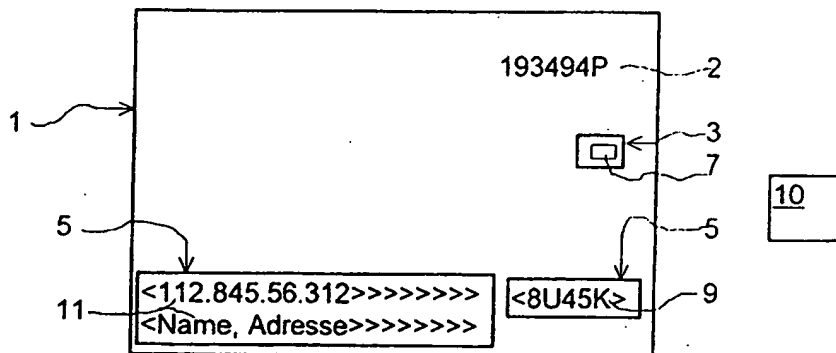


(51) Internationale Patentklassifikation ⁷ : B42D 15/10	A1	(11) Internationale Veröffentlichungsnummer: WO 00/38932 (43) Internationales Veröffentlichungsdatum: 6. Juli 2000 (06.07.00)
--	-----------	--

(21) Internationales Aktenzeichen: PCT/EP99/10141 (22) Internationales Anmeldedatum: 20. Dezember 1999 (20.12.99) (30) Prioritätsdaten: 2557/98 24. Dezember 1998 (24.12.98) CH (71) Anmelder (für alle Bestimmungsstaaten ausser US): OVD KINEGRAM AG [CH/CH]; Gubelstrasse 22, CH-6301 Zug (CH). (72) Erfinder; und (75) Erfinder/Anmelder (nur für US): TOMPKIN, Wayne, Robert [CH/CH]; Oesterliwaldweg 2, CH-5400 Baden (CH). STAUB, René [CH/CH]; Schmiedstrasse 6, CH-6330 Cham (CH). (74) Anwalt: SIEMENS BUILDING TECHNOLOGIES AG; Corporate Intellectual Property Rights, Gubelstrasse 22, CH-6300 Zug (CH).	(81) Bestimmungsstaaten: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO Patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG). Veröffentlicht <i>Mit internationalem Recherchenbericht.</i> <i>Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist: Veröffentlichung wird wiederholt falls Änderungen eintreffen.</i>
---	--

(54) Title: ACTIVABLE DOCUMENT AND SYSTEM FOR AKTIVABLE DOCUMENTS

(54) Bezeichnung: AKTIVIERBARES DOKUMENT UND SYSTEM FÜR AKTIVIERBARE DOKUMENTE



(57) Abstract

A document (1) has the following features on a substrate (6): at least one document number (2); an optical marking (3) with a machine-readable code (7); and a storage field (4) for accommodating a control number (9). The control number (9) is generated from at least one of the document number (2), the code (7) and a first secret key (10) by means of a cryptographic operation when the document is supplied to an authorised person and entered into the storage field (4). The authenticity of a certificate of authenticity produced in this way can be checked with a verifier, using a cryptographic operation and the information stored on the document (1) by means of a second key.

(57) Zusammenfassung

Ein Dokument (1) weist auf dem Substrat (6) wenigstens eine Dokumentennummer (2), eine optische Markierung (3) mit einer maschinell lesbaren Kennung (7) und ein Speicherfeld (4) für die Aufnahme einer Kontrollnummer (9) auf. Die Kontrollnummer (9) wird erst im Moment der Abgabe an eine berechnete Person mittels einer kryptographischen Operation aus wenigstens der Dokumentennummer (2), der Kennung (7) und einem ersten geheimen Schlüssel (10) erzeugt und in das Speicherfeld (4) eingeschrieben. Ein derart erzeugtes Echtheitszertifikat ist mit einem Verifikator unter Verwendung einer kryptographischen Operation und der auf dem Dokument (1) gespeicherten Information mittels eines zweiten Schlüssels auf seine Echtheit überprüfbar.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidshan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland	ML	Mali	TR	Türkei
BG	Bulgarien	HU	Ungarn	MN	Mongolei	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MR	Mauretanien	UA	Ukraine
BR	Brasilien	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Island	MX	Mexiko	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	NE	Niger	UZ	Usbekistan
CF	Zentralafrikanische Republik	JP	Japan	NL	Niederlande	VN	Vietnam
CG	Kongo	KE	Kenia	NO	Norwegen	YU	Jugoslawien
CH	Schweiz	KG	Kirgisistan	NZ	Neuseeland	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	PL	Polen		
CM	Kamerun	KR	Republik Korea	PT	Portugal		
CN	China	KZ	Kasachstan	RO	Rumänien		
CU	Kuba	LC	St. Lucia	RU	Russische Föderation		
CZ	Tschechische Republik	LI	Liechtenstein	SD	Sudan		
DE	Deutschland	LK	Sri Lanka	SE	Schweden		
DK	Dänemark	LR	Liberia	SG	Singapur		
EE	Estland						

Aktivierbares Dokument und System für aktivierbare Dokumente

Die Erfindung bezieht sich auf ein aktivierbares Dokument gemäss dem Oberbegriff des Anspruchs 1 und auf ein System für aktivierbare Dokumente gemäss dem Oberbegriff des Anspruchs 9.

Solche aktivierbare Dokumente sind für persönliche Ausweise verwendbar, wie z.B. Bankschecks.

- 5 Pässe, Identitätskarten, Abonnements, Billette, Gesundheitskarten, Kreditkarten, IC-Karten, elektronische Geldbörsen (smart cards), Wertdokumente usw. Ein solches System, das aktivierbare Dokumente verwendet, sind vor allem bei Echtheitskontrollen und/oder Inhaber - Kontrollen der Dokumente verwendbar.

- 10 Zur Sicherung der genannten Dokumente werden visuell leicht erkennbare Hologramme und andere Beugungsstrukturen eingesetzt, wobei sie meist in Form von Etiketten aus einem die beugungsoptisch wirksamen Strukturen schützenden Kunststofflaminat mit dem Substrat des Dokuments unlösbar verbunden sind (EP 0 330 738 A1). An und für weisen solche Dokumente einen sehr hohen Sicherheitsstandard gegen Fälschungen oder Verfälschungen auf.

- 15 Aus der EP 0 713 197 A1 ist ein Datenträger in Kartenform mit einer in den Kartenkörper integrierten elektronischen Schaltung und einer optischen Markierung bekannt, wobei der Inhalt der elektronischen Schaltung mit der Information der optischen Markierung verknüpft ist. Als optische Markierungen können beispielsweise mit Farbe aufgebrachte Zeichen, wie ein Barcode oder Schriftzeichen, oder beugungsoptisch wirksame Strukturen, wie sie in der CH - PS 653 161 A5, in der EP 0 366 858 A1, in der EP 0 718 795 A1, in der EP 0 883'085 A1 usw. verwendet werden. In den genannten Schriften sind
20 auch Ausführungen von Lese- und Schreibgeräten für die optischen Markierungen beschrieben.

- Schliesslich beschreibt die US - PS 3 833 795 die Sicherung der Echtheit von seriell nummerierten Dokumenten (Banknoten, Wertpapiere). Eine solches Dokument trägt zwei Nummernfelder, das eine ist für eine fortlaufende Nummerierung der Dokumente, der Identitätsnummer, vorgesehen, das andere ist eine bei der Ausgabe zufällig gewählte Kontrollnummer, die in eine zentral geführte Liste eingetragen
25 wird. Ein ausgegebenes Dokument wird anhand der externen Liste oder mittels eines Listen - Algorithmus überprüft, wobei eine Leseeinrichtung zunächst die Identitätsnummer und die Kontrollnummer abliest und anschliessend die Kontrollnummer der Identitätsnummer auf dem Dokument mit der von der Leseeinrichtung mittels der externen Liste oder des Listen - Algorithmus gefundenen Kontrollnummer vergleicht. Dieses Dokument ist jedoch nicht gegen Kopieren geschützt.

- 30 Ein grosses Problem stellt jedoch die Sicherheit der Dokumente im Zeitraum von der Herstellung bis zur Übergabe des Dokuments an die berechtigte Person dar, da in diesem Zeitraum die Dokumente auf dem Transport gestohlen werden können, um mit diesen Dokumenten unberechtigte Personen auszurüsten.

Der Erfindung liegt die Aufgabe zugrunde, ein in grossen Mengen kostengünstig hergestelltes, gegen Kopieren geschütztes Dokument derart zu sichern, dass seine Echtheitsmerkmale erst beim Inverkehrbringen vervollständigt werden und die Echtheitsmerkmale einfach und kostengünstig maschinell zu überprüfen sind.

- 5 Die genannte Aufgabe wird erfindungsgemäss durch die im Kennzeichen der Ansprüche 1 und 9 angegebenen Merkmale gelöst. Vorteilhafte Ausgestaltungen der Erfindung ergeben sich aus den abhängigen Ansprüchen.

Ausführungsbeispiele der Erfindung sind in der Zeichnung dargestellt und werden im folgenden näher beschrieben.

- 10 Es zeigen: Figur 1 ein Dokument,
Figur 2 ein aktiviertes Dokument,
Figur 3 eine IC - Karte als Dokument,
Figur 4 einen Informationsstreifen,
Figur 5 ein System,
15 Figur 6 ein Validiergerät und
Figur 7 einen Verifikator.

- In der Figur 1 bedeutet 1 ein Dokument, 2 Dokumentennummer, 3 eine optische Markierung, 4 ein Speicherfeld, 5 ein Kontrollfeld und 6 ein Substrat. Das Dokument 1 besitzt ein Substrat 6 aus Papier, Kunststoffflies, Kunststoffolie, einem Schichtverbund aus Kunststoff, Lacken und/oder Papier usw. Die
20 beiden Oberflächen des Substrats 6 können bedruckt sein, wie dies bei Bankschecks, Pässen, Identitätskarten, Abonnements, Billetts, Gesundheitskarten, Kreditkarten, IC-Karten, elektronische Geldbörsen (smart cards), Wertdokumente, Banknoten usw. üblich ist, und weisen wenigstens auf einer Seite die wenigstens maschinell lesbare Dokumentennummer 2 auf. Die Dokumentennummer 2 kann in
25 Klarschrift und/oder als Strichkode in bekannter Art mit normaler, fluoreszierender oder magnetischer Tinte auf das Substrat 6 aufgebracht sein. Für die optische Markierung 3 sind beispielsweise mit
normaler, fluoreszierender oder magnetischer Farbe aufgebrachte oder mittels Perforieren des Substrats 6 erzeugte Zeichen, wie ein Barcode, Schriftzeichen usw., oder beugungsoptisch wirksame
Strukturen verwendbar. Die optische Markierung 3 enthält eine digitale Information, eine Kennung 7.
Von besonderem Vorteil ist die Verwendung der optischen Markierung 3 mit beugungsoptisch
30 wirksamen Strukturen wegen ihrer hohen Sicherheit gegen Fälschung und Kopieren. Sie sind aus den eingangs genannten Schriften CH 653 161 A5, EP 0 366 858 A1, EP 0 718 795 A1 usw. bekannt und eignen sich besonders zum maschinellen Ablesen einer in der beugungsoptischen Markierung 3

enthaltenen Kennung 7. Die Kennung 7 beinhaltet Informationen über die Art des Dokuments, die Dokumentserie usw. nicht aber über die Dokumentennummer 2, die das Dokument 1 innerhalb einer Serie identifiziert, d.h. die Dokumente 1 einer Serie sind kostengünstig herstellbar und unterscheiden sich nur durch die beispielsweise aufgedruckten Dokumentennummern 2. Die Grösse der optischen Markierung 3 ist durch die darin enthaltene Kennung 7 bestimmt und die benötigte Fläche umfasst typisch ungefähr 1 mm^2 . Extremwerte für diese Fläche dürften bei $0,1 \text{ mm}^2$ eine untere und bei 1 cm^2 eine obere Grenze erreichen. Die optische Markierung 3 kann auch visuell unsichtbar in einer transparenten Folie gemäss CH 653 161 A5 eingebracht sein oder auch unauffällig innerhalb eines Hologramms oder eines beugungsoptischen Musters, einem Sicherheitsmerkmal 8, beispielsweise gemäss CH 659 433 A5, verborgen sein. Das Sicherheitsmerkmal 8 dient der Identifizierung des Dokuments 1 für den Mann auf der Strasse und wirkt auf dem Dokument 1 sehr auffällig.

Das Speicherfeld 4 und das Kontrollfeld 5 bleiben zur Auslieferung an die Inverkehrbringer (Verkaufsstellen, Ausgabestellen, Bankschalter usw.) leer. Ohne eine in der Figur 2 gezeigte

Kontrollnummer 9 im Speicherfeld 4 ist das Dokument 1 unbrauchbar. Beim Inverkehrbringen müssen die Dokumente 1 durch eine Aktivierung ihre Gültigkeit erlangen. Beispielsweise werden die Dokumentennummer 2 und die Kennung 7 maschinell aus dem Dokument 1 abgelesen. Wenigstens diese Informationen werden mit einem ausserhalb des Dokuments vorhandenen ersten geheimen Schlüssel 10 in einer kryptographischen Operation miteinander verknüpft und aus dem Resultat die dem Dokument 1 zugehörige Kontrollnummer 9 erzeugt und in das Speicherfeld 4 eingeschrieben. Das

Dokument 1 ist erst jetzt vollständig und seine Gültigkeit ist anhand der Dokumentennummer 2, der Kennung 7 und der Kontrollnummer 9 überprüfbar. Bei bestimmten Dokumentarten ist während der Aktivierung auch die Beschriftung des Kontrollfelds 5 vorgesehen. Der Inhalt des Kontrollfelds 5 umfasst wenigstens visuell lesbare, individuelle, auf eine Person, Veranstaltung, Firma, usw. bezogene Informationen, wie Name, Anschrift, Sozial- oder andere Versicherungsnummer, Staatszugehörigkeit, Zeitangaben, Geldbetrag usw. Diese Informationen, im folgenden Kode 11 genannt, können auch zusammen mit der Dokumentennummer 2, der Kennung 7 mit der kryptographischen Operation zur Kontrollnummer 9 verarbeitet werden.

In einer Ausführung des Dokuments 1 ist nach einem der bekannten Verfahren das Speicherfeld 4 und/oder das Kontrollfeld 5 mit der Kontrollnummer 9 bzw., dem Kode 11 in maschinenlesbarer Druckschrift beschriftet. Diese Klarschrift, z.B. OCR - Schrift, ist sowohl visuell als auch maschinell lesbar. Anstelle oder zusammen mit der Druckschrift kann die Kontrollnummer 9 auch als Strichkode, der im Detailhandel weit verbreitet ist, dargestellt sein.

In der Figur 3 ist eine weitere Ausführung des Dokuments 1 in Form einer Karte (Gesundheitskarte, Kreditkarte, IC-Karte, Smartcards, usw) gezeigt. In das Substrat 6 ist ein an sich bekanntes Modul 12

mit einem der Mikrochip 13 eingelassen, in dessen Speicher 14 das Speicherfeld 4 eingerichtet ist. Das Speicherfeld 4 kann nur einmal mit der Kontrollnummer 9 beim Aktivieren des Dokuments 1 mittels einer über ein Kontaktfeld 15 gesandte elektronischen Signalfolge beschrieben werden, eine spätere Veränderung ist nicht mehr möglich. Wie in der eingangs erwähnten EP 0 713 197 A1 kann die

5 Signalfolge auch mittels hier nicht gezeigten induktiven oder optischen Mitteln an ein entsprechend gestaltetes Modul 12 des Dokuments 1 übertragen werden.

Eine andere Ausführung des Dokuments 1 in Kartenform weist auf dem Substrat 7 einen Magnetstreifen 16 auf. Die Kontrollnummer 9 (Figur 2) und der Kode 11 (Figur 2) wird beim Aktivieren des Dokuments 1 magnetisch kodiert in das Speicherfeld 4 bzw. in das Kodierfeld 5 auf dem

10 Magnetstreifen 16 eingezeichnet. Das Speicherfeld 4 weist nach der Aktivierung im Speicherfeld 4 wenigstens die magnetisch lesbare Kontrollnummer 9 auf.

Eine weitere Ausführung des Dokuments 1 weist im Speicherfeld 4 einen mit dem Substrat 6 während des Herstellungsprozesses des Dokuments 1 aufgebracht, in der Figur 4 dargestellten beugungsoptischen Informationsträger 17 auf, wie er in der eingangs genannten Schrift EP 0 718 795

15 A1 beschrieben ist. Der Informationsträger 17 weist im unbeschriebenen Zustand 17' wenigstens eine Reihe von in Paaren 19 angeordneten Beugungsfeldern 18, wobei sich die beiden mikroskopischen Beugungsstrukturen eines Paares 19 in wenigstens einem Gitterparameter unterscheiden. Während des Aktivierens wird die Kontrollnummer 9 als digitale Folge auf dem Informationsträger 17 abgebildet, wobei beim Beschreiben entsprechend dem Bitwert in jedem Paar eines der beiden Beugungsfelder 18

20 die Beugungsstruktur durch Zuführen von Wärmeenergie zerstört oder die Beugungsstruktur durch Abdecken, z.B. mit einem nicht transparenten Decklack, unwirksam gemacht wird. Im Informationsträger 17'' ist nach der Aktivierung bei jedem Paar eine der beiden Beugungsstrukturen nicht mehr beugungsoptisch wirksam. Das Speicherfeld 4 weist nun die Kontrollnummer 9 in optisch maschinell leicht lesbaren Zeichen auf. Der Vorteil dieses Informationsträgers 17 ist, dass er nur einmal

25 beschrieben werden kann. Jede weitere Veränderung des Informationsträgers 17 ist maschinell leicht zu erkennen.

In einer Ausführung des Dokuments 1 ist die optische Markierung 3 und die Kontrollnummer 9 mit Beugungsstrukturen ausgeführt und auf dem gleichen Informationsträger 17 untergebracht. Der Vorteil dieser Ausführung ist, dass mit einem einzigen optischen Leser 26 gemäss der EP 0 718 795 A1 das

30 Auslesen der Kennung 7 und der Kontrollnummer 9 sowie das Beschriften des Informationsträgers 17 durchgeführt wird. Das teure Sicherheitsmerkmal 8 (Figur 1) kann weggelassen werden.

Die Beschriftungen 2, 9, 11, das Modul 12 und der Magnetstreifen 16 können an sich beliebig auf den beiden Seiten des Dokuments 1 verteilt sein, wobei üblicherweise nur der Magnetstreifen 16 auf der Rückseite des Substrats 6 angeordnet ist.

Die Figur 5 zeigt ein System 20, das sich für die Verwendung der vorstehend beschriebenen Dokumente 1 eignet. Das System 20 umfasst wenigstens ein Dokument 1, ein Validiergerät 21 für die Aktivierung des Dokuments 1 und einen Verifikator 22, mit dem eine Echtheitskontrolle des Dokuments 1 durchzuführen ist. Während die Validiergeräte 21 bei den wenigen Inverkehrbringern aufgestellt sind, muss eine Vielzahl von einfach zu bedienenden, möglichst autonomen Verifikatoren 22 dort im Einsatz sein, wo auch immer solche Dokumente 1 einer Echtheitskontrolle unterzogen werden.

Die vom Hersteller angelieferten Dokumente 1 mit der Dokumentennummer 2 werden bei den Inverkehrbringern gelagert bis eines der Dokumente 1 einer berechtigten Person zugeteilt wird, wobei mittels des Validiergerätes 21 das dieser Person zugeteilte Dokument 1 durch Einschreiben der Kontrollnummer 9 in das Speicherfeld 4 zu einem Echtheitszertifikat 23 vervollständigt wird.

Eine Ausführung des Validiergeräts 21 gemäss Figur 6 umfasst eine Recheneinheit 24, eine Transportvorrichtung 25 für das Dokument 1, einen optischen Leser 26 zum maschinellen Auslesen der Kennung 7 (Figur 1) auf der optischen Markierung 3 des nicht aktivierten Dokuments 1 sowie ein Aufzeichnungsmittel 27. Weitere in der Zeichnung der Figur 6 gestrichelt eingezeichnete, fakultative Leseeinheiten 29 ermöglichen ein Ablesen der Dokumentennummer 2 (Figur 1), der Kontrollnummer 9 (Figur 2) und des Codes 11 (Figur 2). Die Leseeinheiten 29 unterscheiden sich entsprechend der für das System 20 einmal gewählten Aufzeichnungstechniken, die für die Dokumentennummer 2, für die Kontrollnummer 9 und für den Code 11 vorbestimmt sind. Die Transportvorrichtung 25, der optische Leser 26, das oder die Aufzeichnungsmittel 27 und die Leseeinheiten 29 sind mit der Recheneinheit 24 verbunden.

Die Recheneinheit 24 ist über Leitungen mit der Transportvorrichtung 25, dem optischen Leser 26, und mit dem Aufzeichnungsmittel 27 verbunden, steuert diese Geräte 25, 26, 27 und empfängt die von diesen Geräten 25, 26, 27 ausgesandte Informationen, damit das Dokument 1 maschinell abgelesen und beschriftet werden kann. Die Recheneinheit 24 weist wenigstens ein Sicherheitsmodul 30 auf, das in einer integrierte Schaltung einen Mikroprozessor mit zugehörigen Speicherplätzen umfasst. Der Mikroprozessor führt kryptographische Operationen aus und benutzt dazu den in den Speicherplätzen enthaltenen ersten geheimen Schlüssel 10.

Die Transportvorrichtung 25 bewirkt in einer Ausführung eine Relativbewegung zwischen dem Dokument 1 einerseits und den Lesemitteln 26, 29 und dem Aufzeichnungsmittel 27 andererseits. In der Figur 6 wird das Dokument 1 gegenüber den feststehenden Lesemitteln 26, 29 und dem Aufzeichnungsmittel 27 bewegt. Für die Transportvorrichtung 25 sind unterschiedliche, an sich bekannte Ausführungen für Blätter oder für Karten bekannt und einsetzbar. Auf eine aufwendige Transportvorrichtung 25 kann verzichtet werden, wenn die optische Markierung 3 bzw. das

Sicherheitselement 8 (Figur 1) gemäss der Lehre in der EP 0 883'085 A1 gestaltet ist und das Beschriften des Speicherfelds 4 manuell erfolgt.

Das Aufzeichnungsmittel 27 ist zum Einschreiben der Kontrollnummer 9 und des Kodes 11 in das Speicherfeld 4 bzw. Kodierfeld 5 eingerichtet und benutzt die für das Dokument 1 vorgesehene

- 5 Aufzeichnungstechnik, beispielsweise ein Druck-, Tintenstrahl-, Xerographie-, Perforations- usw. Verfahren, ein in der EP 0 718 795 A1 beschriebenes Schreibverfahren für die Informationsträger 17, eine magnetische Aufzeichnung oder die elektronische Speicherung im Speicher 14 (Figur 3). Die Kontrollnummer 9 kann auch manuell in das Speicherfeld 4 mit dokumentechter Tinte eingeschrieben werden. Das Perforationsverfahren für Dokumente 1 ist z.B. im DE Gebrauchsmuster G 93 15 294.9
- 10 beschrieben.

Die Tastatur 28 ist ganz allgemein eine Eingabevorrichtung für aus Ziffern oder alphanumerische Zeichen bestehende Informationen. Die Eingabevorrichtung kann auch über einen Anschluss 28' an ein Telefon- oder Computernetzwerk 37 (Figur 5) mit dem Validiergerät 21 verbunden sein, insbesondere können die den Code 11 bildenden Informationen von einer Zentralstelle abgerufen werden.

- 15 Die Leseinheit 29 ist der für das Dokument 1 verwendeten Aufzeichnungstechnik angepasst. Die Leseinheit 29 ist z.B. ein Klargrifleser, ein Barcodeleser usw. für visuell lesbare Zeichen, aus denen sich die Dokumentennummer 2, die Kontrollnummer 9 und den Code 11 zusammensetzen. Diese Leseinheiten 29 tasten mit einem Lichtstrahl Teile oder das ganze Dokument 1 ab und messen die Intensität des vom Dokument 1 zurückgestreuten Lichts. Die für die magnetisch aufgezeichnete
- 20 Informationen bzw. zum elektronischen Auslesen aus dem Speicher 14 geeignete Leseinheit 29 ist allgemein bekannt.

Der Aufbau und Arbeitsweise des optischen Lesers 26 und für eine Leseinheit 29, die zum Auslesen der Kontrollnummer 9 aus dem optischen Informationsträger 17 (Figur 4) befähigt ist, sind beispielsweise aus den eingangs genannten Schriften CH - PS 653 161 A5, EP 0 366 858 A1,

- 25 EP 0 718 795 A1, EP 0 883'085 A1 bekannt.

In einer kostengünstigen Ausführung zur Aktivierung liest ein Bediensteter eines nicht aktivierten Dokuments 1 dessen Dokumentennummer 2 visuell ab und gibt die Dokumentennummer 2 (Figur 2) über eine Tastatur 28 manuell in die Recheneinheit 24 ein. Anschliessend wird das Dokument 1 in die auf einen Kanal oder eine Plattform reduzierte Transportvorrichtung 25 unter den optischen Leser 26 gesteckt bzw. gelegt, damit der optische Leser 26 die Kennung 7 ablesen und der Recheneinheit 24 übermitteln kann. Die Recheneinheit 24 verschlüsselt die Kennung 7 und die Dokumentennummer 2 mit dem ersten geheimen Schlüssels 10 und bildet eine digitale Signatur, die Kontrollnummer 9, auf einer Anzeige 31 ab. Der Bedienstete überträgt nun manuell die Kontrollnummer 9 in das Speicherfeld 4 auf dem Dokument 1, das nun damit aktiviert zum Elektronenlesen ist.

Speicherfeld 4 kann in Felder für je ein Zeichen der Kontrollnummer 9 eingeteilt sein, um ein maschinelles Lesen der handschriftlich eingetragenen Kontrollnummer 9 zu erleichtern.

Eine zweite Ausführung weist eine in der Zeichnung der Figur 6 punktiert gezeichnete Lesereinheit 29 auf, die die Dokumentennummer 2 maschinell direkt vom Dokument 1 abliest und an die

- 5 Recheneinheit 24 abgibt. Die Recheneinheit 24 verschlüsselt wenigstens die Kennung 7 und die Dokumentennummer 2 mit dem ersten geheimen Schlüssels 10 zur Kontrollnummer 9. Anschliessend überträgt das Aufzeichnungsmittel 27 die Kontrollnummer 9 in den Speicherfeld 4 in der vom System 20 vorbestimmten Technik.

- Das Validiergerät 21 ist in einer dritten Ausführung zusätzlich mit der Tastatur 28 und der Anzeige 31
10 ausgestattet, um über die Tastatur 28 den Kode 11 einzugeben, wobei die Anzeige 31 zur Kontrolle des Kodes 11 dient. Der Kode 11 wird ebenfalls mit dem Aufzeichnungsmittel 27 auf das Dokument 1 übertragen. Für besonders wichtige Dokumente 1 ist das Validiergerät 21 dazu eingerichtet, die Eingabe einer persönlichen Identifikationsnummer (PIN) vom Benutzer zu verlangen. Diese PIN identifiziert in einem Fall als Zulassungs - PIN den Bediensteten, der das Validiergerät 21 bedient, und in einem
15 zweiten Fall als Inhaber - PIN den Dokumentinhaber, wobei bei der Aktivierung des Dokuments 1 der Inhaber seine PIN über die Tastatur 28 eintippt und im Rechengerät 24 die Inhaber - PIN zusammen mit dem Kode 11 oder allein als Parameter für die Erzeugung der Kontrollnummer 9 dient.

- In einer vierten Ausführung des Validiergeräts 21 ist anstelle des optischen Lesers 26 und der
20 Leseinheit 29 ein einziger Leser 26 so eingerichtet, dass er sowohl die optische Markierung 3 und die Dokumentennummer 9 erkennen kann.

In einer fünften Ausführung ist das Validiergerät 21 auch zum Erkennen der Kontrollnummer 9 eingerichtet. Somit ist das Validiergerät 21 fähig, aktivierte und nicht aktivierte Dokumente 1 zu unterscheiden und zusätzlich die Kontrollnummer 9 auf ihre Richtigkeit zu überprüfen.

- Die Kontrollnummer 9 ist das Ergebnis der kryptographischen Operation in der Recheneinheit 24, einer
25 mathematischen Funktion f:

Kontrollnummer 9 = f(Dokumentennummer 2, Kennung 7, erster geheimer Schlüssel 10) bzw.

Kontrollnummer 9 = f(Dokumentennummer 2, Kennung 7, Kode 11, erster geheimer Schlüssel 10).

- Da sich die Systeme 20 nicht nur in der Aufzeichnungstechnik sondern auch in der Anzahl und Art der Parameter der kryptographischen Operation unterscheiden, werden, zwecks einfacherer Beschreibung,
30 nachfolgend die für die Erzeugung der Kontrollnummer 9 auf dem Dokument 1 vorhandenen Werte, wie Dokumentennummer 2, Kennung 7, Kode 11 und die getrennt vom Dokument 1 gespeicherte Inhaber - PIN, als Parameter der kryptographischen Operation bezeichnet, wobei darunter wenigstens die Dokumentennummer 2 und die Kennung 7 zu verstehen sind, allenfalls ergänzt um den Kode 11

und/oder die Inhaber - PIN. Ein System 20 ist somit durch die verwendeten Aufzeichnungstechniken, die Ausführung des Dokuments 1, die Parameter der kryptographischen Operation und dem ersten geheimen Schlüssel 10 bestimmt.

Weder der erste geheime Schlüssel 10 noch der Algorithmus sind der Öffentlichkeit bekannt und werden von einer "certification authority" in einem Sicherheitsmodul 30 zum Einsetzen in die Recheneinheit 23 abgegeben. Nachdem die Recheneinheit 24 die Parameter der Funktion f in das Sicherheitsmodul 30 eingegeben sind, erzeugt das leicht auswechselbare Sicherheitsmodul 30 direkt die Kontrollnummer 9 oder ein Zwischenresultat, das für die Berechnung der Kontrollnummer 9 in der Recheneinheit 24 dient.

Der erste geheime Schlüssel 10 dient sowohl für die kryptographischen Operation zum Erzeugen der Kontrollnummer 9 als auch für die Überprüfung der Richtigkeit der Kontrollnummer 9 in Kenntnis der auf dem Dokument 1 vorhandenen Informationen.

Der Verifikator 22 in der Figur 7 weist bis auf das Aufzeichnungsmittel 27 (Figur 6) gleiche Komponenten wie das Validiergerät 21 (Figur 6) auf. Die Ausführungen des Verifikator 22 unterscheiden sich in den Leseinheiten 29, die sich entsprechend der für das System 20 (Figur 5) gewählten Aufzeichnungstechnik unterscheiden. Der Verifikator 22 umfasst in der kostengünstigen Ausführung wenigstens ein Aufnahmemittel 32 für ein zu überprüfendes Echtheitszertifikat 23 (Figur 5), ein Rechengerät 33 mit dem Sicherheitsmodul 30, den optischen Leser 26 für die Kennung 7, die Tastatur 28 und die Anzeige 31. Das Rechengerät 33 ist mit dem optischen Leser 26, der Tastatur 28 und der Anzeige 31 verbunden. Das Rechengerät 33 überprüft mit einer anderen kryptographischen Operation, ob die Kontrollnummer 9 (Figur 2) zu den Parametern der kryptographischen Operation, die wenigstens die Dokumentnummer 2 und die Kennung 7 umfassen, passt. Dazu verwendet das Rechengerät 33 einen zweiten Schlüssel 34, der im Sicherheitsmodul 30 mit dem entsprechenden Algorithmus enthalten ist. Das Rechengerät 33 kann mit der anderen kryptographischen Operation keine Verschlüsselungen wie die Recheneinheit 24 (Figur 6) im Validiergerät 21 vornehmen. Die Verwendung des zweiten Schlüssels 34, der vom ersten Schlüssel 10 völlig verschieden ist, weist den Vorteil auf, dass die sich aus der Verwendung ergebenden weiten Verbreitung der Verifikatoren 22 ergebenden Schwierigkeit der Geheimhaltung des zweiten Schlüssels 34 für die Sicherheit des Systems 20 irrelevant ist. Das Rechengerät 32 stellt das Ergebnis der Echtheitskontrolle auf der Anzeige 31 dar.

Für eine Echtheitskontrolle liest ein Kontrolleur visuell die Parameter der kryptographischen Operation, wenigstens die Dokumentnummer 2 und die Kennung 7, auf dem Echtheitszertifikat 23 und die Kontrollnummer 9 im Speicherfeld 4 ab und führt dem Rechengerät 33 die abgelesenen Zeichenfolgen über die Tastatur 28 zu. Das Aufnahmemittel 32 kann auch eine einfache Plattform unter dem optischen Leser 26 sein, auf die der Kontrolleur das Dokument 1 so auflegt, dass die optische Markierung 3 im

Bereich des optischen Lesers 26 ist. Die maschinell gelesene Kennung 7 gelangt direkt in das Rechengerät 33. Das Ergebnis der Echtheitskontrolle erscheint auf der Anzeige 31. Im einfachsten Fall besteht die Anzeige 31 aus zwei Signallampen um das Ja/Nein - Ergebnis der Echtheitskontrolle darzustellen. Jedoch ist es von Vorteil, wenn die Anzeige 31 sowohl die über die Tastatur 28
5 eingegebenen Parameter und Kontrollzahl 9 sowie das Ja/Nein - Ergebnis anzeigt.

Der Verifikator 22 gibt in einer anderen Ausführung ein Erlaubnissignal über eine Signalleitung 35 an eine Dienstleistungseinrichtung 36 ab. Das Eintreffen des Erlaubnissignals gibt die Dienstleistung der Dienstleistungseinrichtung 36 frei, z.B. Türöffnung, Geldausgabe, Warenbezug, Registrierung usw.

Eine andere Ausführung des Verifikators 22 weist als Aufnahmemittel 32 ein Transportsystem für blatt-
10 oder kartenförmige Dokumente 1 auf. Mit dem Rechengerät 33 ist das vom Rechengerät 33 gesteuerte Aufnahmemittel 32 und zusätzlich zum optischen Leser 26 wenigstens eine Leseinheit 29 zum Übermitteln von Informationen verbunden. Die Leseinheit 29 liest einen oder mehrere Parameter der kryptographischen Operation maschinell aus. Eine Tastatur 28 erübrigt sich für diese Ausführung. Eine Leseinheit 29 ist dann ausreichend, wenn die Parameter der kryptographischen Operation und die
15 Kontrollnummer 9 auf dem Echtheitszertifikat 23 in der gleichen Aufzeichnungstechnik ausgeführt sind.

Für ein System 20, bei dem der Inhaber - PIN verwendet wird, ist die Tastatur 28 für den Inhaber vorgesehen, der sich mit der Inhaber - PIN gegenüber dem Verifikator 22 identifiziert. Die über die Tastatur eingegebene Inhaber - PIN wird in der kryptographischen Operation als Parameter zur
20 Überprüfung der Kontrollnummer 9 verwendet.

Wie beim Validiergerät 21 ist auch eine Identifizierung des Kontrolleurs mittels seiner Benutzer - PIN von Vorteil, um die Hürde für potentielle Einbrecher in das System 20 möglichst hoch anzusetzen. Die Eingabe der richtigen Benutzer - PIN über die Tastatur 28 ermöglicht dem Rechengerät 33 den Benutzer zu identifizieren und den Validator 22 zum Einsatz freizugeben.

25 Zur Figur 5 ist noch zu bemerken, dass das System 20 mit Vorteil in ein bidirektionales Telefon- oder Computernetzwerk 37 zum Datenaustausch zwischen den Validiergeräten 21 und den Verifikatoren 22 einerseits und einem Rechner 37 andererseits eingebettet ist. Das Validiergerät 21 ist über den Anschluss 28' mit dem Netzwerk 37 und das Netzwerk 37 über eine Leitung 38 mit dem zentralen Rechner 39 verbunden. Neben dem bereits erwähnten Abruf von Daten aus dem zentralen Rechner 39
30 für den Kode 11 (Figur 2) ermöglicht das Netzwerk 37 im zentralen Rechner 39 eine Negativliste Dokumentennummern 2 von widerrufenen Echtheitszertifikaten 23 anzulegen. Die über das Netzwerk 37 mit dem zentralen Rechner 39 verbundenen Verifikatoren 22 erhalten über eine Datenleitung 40 die regelmässig nachgeführte Negativliste in das Rechengerät 33 (Figur 7) übertragen. Die Negativliste ist in einem Datenspeicher 41 (Figur 7) des Rechengeräts 33 abgelegt, damit auch beim

Ausfall des Netzwerkes 37 widerrufen Echtheitszertifikate 23 von den Verifikatoren 22 erkannt werden.

PATENTANSPRÜCHE

1. Dokument (1) mit einer wenigstens maschinell lesbaren Dokumentennummer (2) auf dem Substrat (6) und einem Speicherfeld (4) für die Aufnahme einer Kontrollnummer (9) dadurch gekennzeichnet, dass auf dem Substrat (6) eine optische Markierung (3) mit einer maschinell lesbaren Kennung (7) angebracht ist, dass das Speicherfeld (4) zur Aufnahme der wenigstens maschinell lesbaren Kontrollnummer (9) eingerichtet ist und dass die Kontrollnummer (9), die das Ergebnis einer kryptographischen Operation mit wenigstens zwei Parametern, der Dokumentennummer (2) und der Kennung (7), und einem ersten geheimen Schlüssel (10) ist, zur Vervollständigung erst bei der Inverkehrbringung als Echtheitszertifikats (23) im Speicherfeld (4) eingesetzt ist.
2. Dokument (1) nach Anspruch 1, dadurch gekennzeichnet, dass die optische Markierung (3) beugungsoptische Strukturen aufweist und dass wenigstens ein Teil der beugungsoptischen Strukturen die maschinell lesbare Kennung (7) enthält.
3. Dokument (1) nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass das Substrat (6) ein Kontrollfeld (5) für die Aufnahme eines wenigstens visuell lesbaren, individuellen und auf eine Person bezogenen Kodes (11) aufweist.
4. Dokument nach Anspruch 1, 2 oder 3, dadurch gekennzeichnet, dass das Speicherfeld (4) auf dem Substrat (6) angeordnet ist und dass nach der Aktivierung die Kontrollnummer (9) im Speicherfeld (4) in wenigstens maschinell lesbaren Zeichen enthalten ist.
5. Dokument (1) nach Anspruch 1, 2, 3 oder 4, dadurch gekennzeichnet, dass im Substrat (6) ein Mikrochip (13) eingelassen ist, dass das Speicherfeld (4) im Speicher (14) des Mikrochips (13) angeordnet ist und dass nach der Aktivierung das Speicherfeld (4) die Kontrollnummer (9) enthält und der einmal eingeschriebene Inhalt des Speicherfelds (4) elektronisch nicht veränderbar ist.
6. Dokument (1) nach Anspruch 1, 2, 3 oder 4, dadurch gekennzeichnet, dass auf dem Substrat (6) ein Magnetstreifen (16) mit dem Speicherfeld (4) angeordnet ist, dass der Magnetstreifen (16) wenigstens das Speicherfeld (4) enthält und dass nach der Aktivierung das Speicherfeld (4) die magnetisch lesbare Kontrollnummer (9) aufweist.
7. Dokument (1) nach Anspruch 1, 2, 3 oder 4, dadurch gekennzeichnet, dass auf dem Substrat (6) ein optischer Informationsträger (17, 17') angeordnet ist, dass der optische Informationsträger (17, 17') wenigstens das Speicherfeld (4) enthält und dass nach der Aktivierung der nicht mehr veränderbare optische Informationsträger (17, 17') im Speicherfeld (4) die Kontrollnummer (9) in optisch lesbaren Zeichen aufweist.
8. Dokument (1) nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass ein Teil des optischen Informationsträgers (17, 17') die optische Markierung (3) bildet und die Kennung (7) enthält

9. System (20) bestehend aus wenigstens einem Dokument (1) nach einem der Ansprüche 1 bis 8, einem Validiergerät (21) und einem Verifikator (22), dadurch gekennzeichnet, dass das Dokument (1) wenigstens eine maschinell lesbare Dokumentennummer (2), eine optische Markierung (3) mit einer maschinell lesbare Kennung (7) und ein wenigstens maschinell lesbares Speicherfeld (4) für die
- 5 Aufnahme einer Kontrollnummer (9) aufweist,
- dass im Validiergerät (21) eine Aufnahmevorrichtung (25) zur Aufnahme des Dokuments (1) und einen optischen Leser (26) zum maschinellen Ablesen von wenigstens der Kennung (7) angeordnet sind, dass im Validiergerät (21) eine Recheneinheit (24) für kryptographische Operationen mit einem ersten
- 10 geheimen Schlüssel (10) zum Erzeugen der Kontrollnummer (9) durch Verschlüsseln von wenigstens zwei Parametern, der Dokumentennummer (2) und der Kennung (7), vorhanden ist, dass ein Aufzeichnungsmittel (27) zum Einschreiben der Kontrollnummer (9) in das wenigstens maschinell
- lesbare Speicherfeld (4) eingerichtet ist,
- dass der Verifikator (22) wenigstens ein Rechengerät (33), einen optischen Leser (26) zum maschinellen Ablesen der Kennung (7) und ein Aufnahmemittel (32) zum Ausrichten eines
- 15 Echtheitszertifikats (23) zum maschinellen Ablesen aufweist, dass der Verifikator (22) das wenigstens mit Eingabe- und Ablesemitteln (26; 28; 29) verbundene Rechengerät (33) für kryptographische Operationen mit einem zweiten Schlüssel (34) enthält und dass das Rechengerät (33) zur Überprüfung der Zusammengehörigkeit wenigstens der Kontrollnummer (9) und den zum Verschlüsseln benutzten Parametern der kryptographischen Operation, die auf dem Echtheitszertifikat (23) enthalten sind, und
- 20 zur Darstellung des Vergleichsergebnisses auf einer Anzeige (31) des Verifikators (22) und/oder zur Erzeugung eines Erlaubnissignals eingerichtet ist.
10. System (20) nach Anspruch 9, dadurch gekennzeichnet, dass der Verifikator (22) eine Tastatur (28) für eine manuelle Eingabe einer persönlichen Identifikationsnummer (PIN) zur Freigabe des Verifikators (22) aufweist und dass der Verifikator (22) zum Überprüfen der persönlichen
- 25 Identifikationsnummer eingerichtet ist.
11. System (20) nach Anspruch 9 oder 10, dadurch gekennzeichnet, dass der Verifikator (22) eine mit dem Rechengerät (33) verbundene Tastatur (28) für eine manuelle Eingabe wenigstens der Dokumentennummer (2) und der Kontrollnummer (9) an das Rechengerät (33) aufweist.
12. System (20) nach einem der Ansprüche 9 bis 11, dadurch gekennzeichnet, dass der
- 30 Verifikator (22) wenigstens eine mit dem Rechengerät (33) verbundene Leseinheit (29) für eine maschinelle Eingabe der Dokumentennummer (2) und der Kontrollnummer (9) an das Rechengerät (33) aufweist.

13. System (20) nach Anspruch 9, dadurch gekennzeichnet, dass das Validiergerät (21) eine mit der Recheneinheit (24) verbundene Tastatur (28) für eine manuelle Eingabe wenigstens der Dokumentennummer (2) an die Recheneinheit (24) aufweist.
14. System (20) nach Anspruch 9 oder 13, dadurch gekennzeichnet, dass das Validiergerät (21) eine mit der Recheneinheit (24) verbundene Leseinheit (29) für eine maschinelle Eingabe der Dokumentennummer (2) an die Recheneinheit (24) aufweist.
15. System (20) nach Anspruch 9, 13 oder 14, dadurch gekennzeichnet, dass das Validiergerät (21) für die Eingabe eines individuellen, auf eine Person bezogenen Kodes (11) mittels der Tastatur (28) eingerichtet ist und, dass das Aufzeichnungsmittel (27) im Validiergerät (21) zum Einschreiben des Kodes (11) in das Kontrollfeld (5) angeordnet ist.
16. System (20) nach einem der Ansprüche 9 bis 15, dadurch gekennzeichnet, dass die Recheneinheit (24) im Validiergerät (21) derart ausgebildet ist, dass bei der Verschlüsselung der Kontrollnummer (9) eine über eine Tastatur (28) eingegebene persönlichen Identifikationsnummer Nummer der berechtigten Person als Parameter für die Erzeugung der Kontrollnummer (9) einbezogen ist und dass der Verifikator (22) das Erlaubnissignal nur dann im Rechengerät (33) erzeugt, wenn bei der Echtheitsprüfung die persönlichen Identifikationsnummer Nummer über die Tastatur (28) des Verifikators (22) dem Rechengerät (33) als Parameter der kryptographischen Operation einbezogen ist.
17. System (20) nach einem der Ansprüche 9 bis 16, dadurch gekennzeichnet, dass wenigstens ein Validiergerät (21) und wenigstens ein Verifikator (22) über ein Netzwerk (28, 38, 40; 37) mit einem zentralen Rechner (39) zum bidirektionalen Datenaustausch verbunden sind.
18. System (20) nach einem der Ansprüche 9 bis 17, dadurch gekennzeichnet, dass das wenigstens ein Verifikator (22) über eine Signalleitung (35) mit einer Dienstleistungseinrichtung (36) verbunden ist und dass die Dienstleistungseinrichtung (36) zum Freigeben einer Dienstleistung mittels des über die Signalleitung (35) an die Dienstleistungseinrichtung (36) gesandten Erlaubnissignals eingerichtet ist.

Fig. 1:

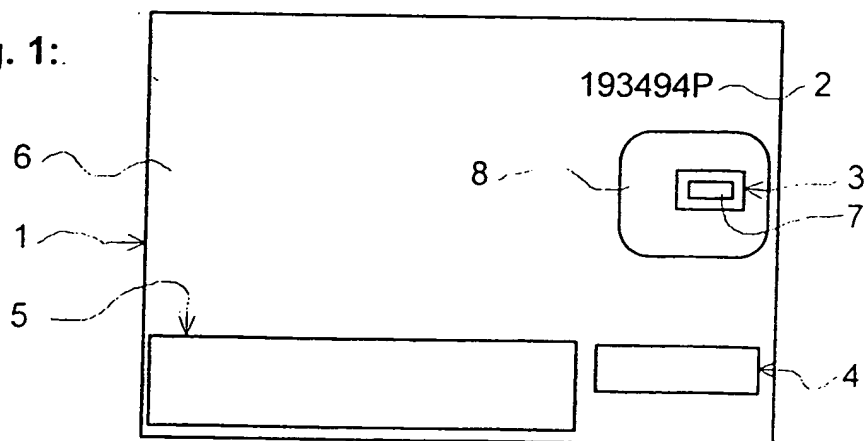


Fig. 2:

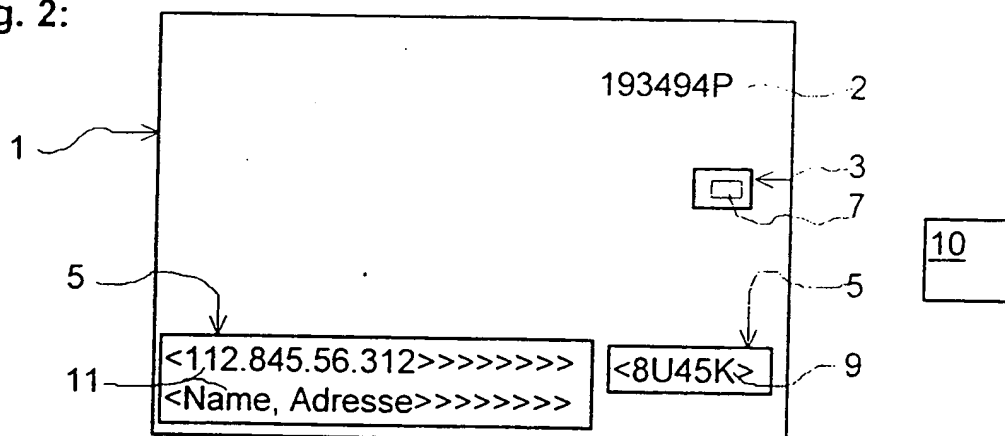


Fig. 3:

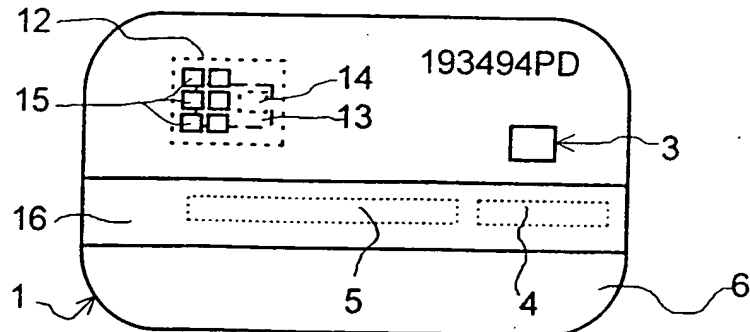


Fig. 4:

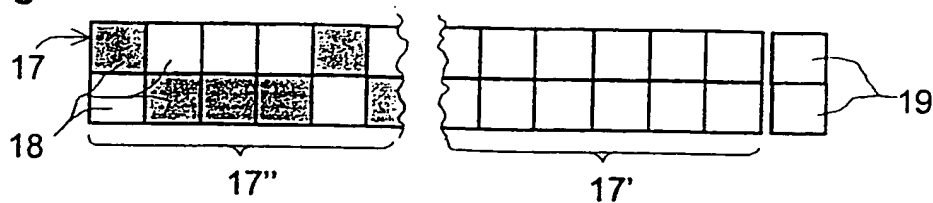


Fig. 5:

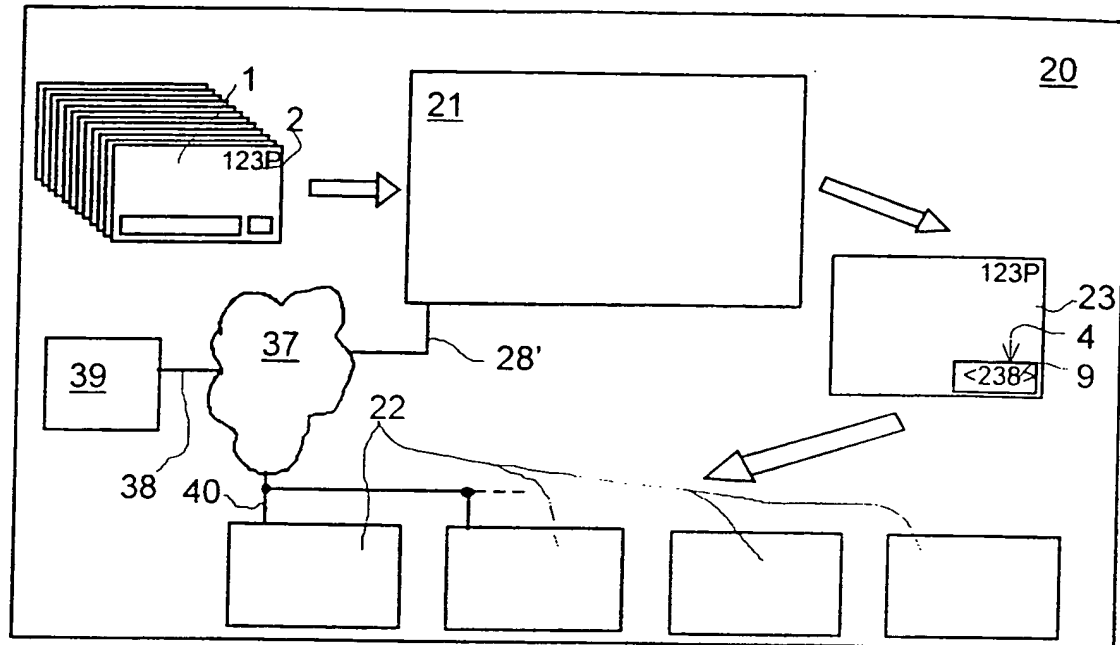


Fig. 6:

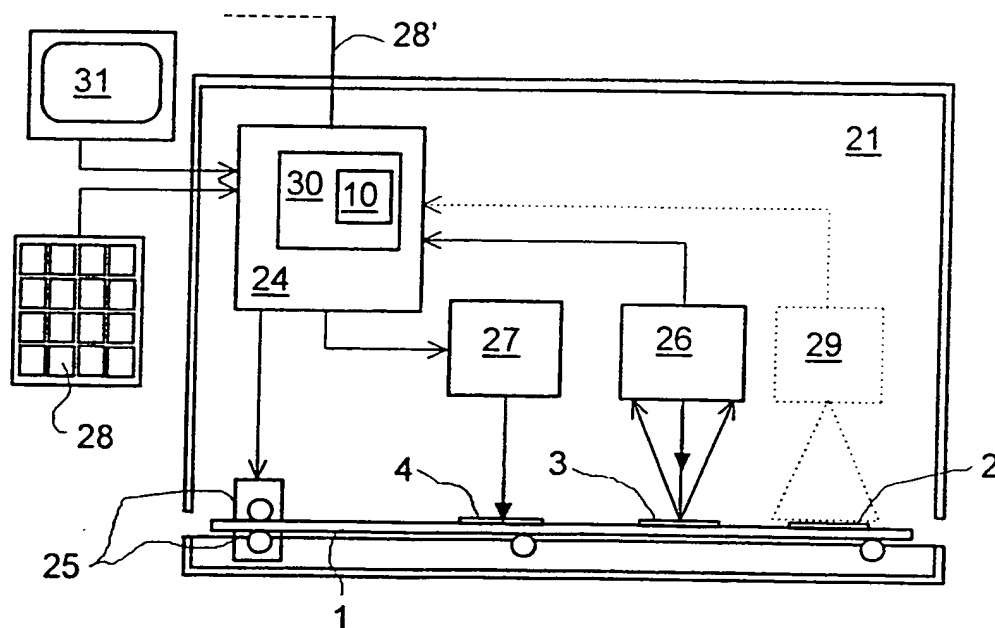
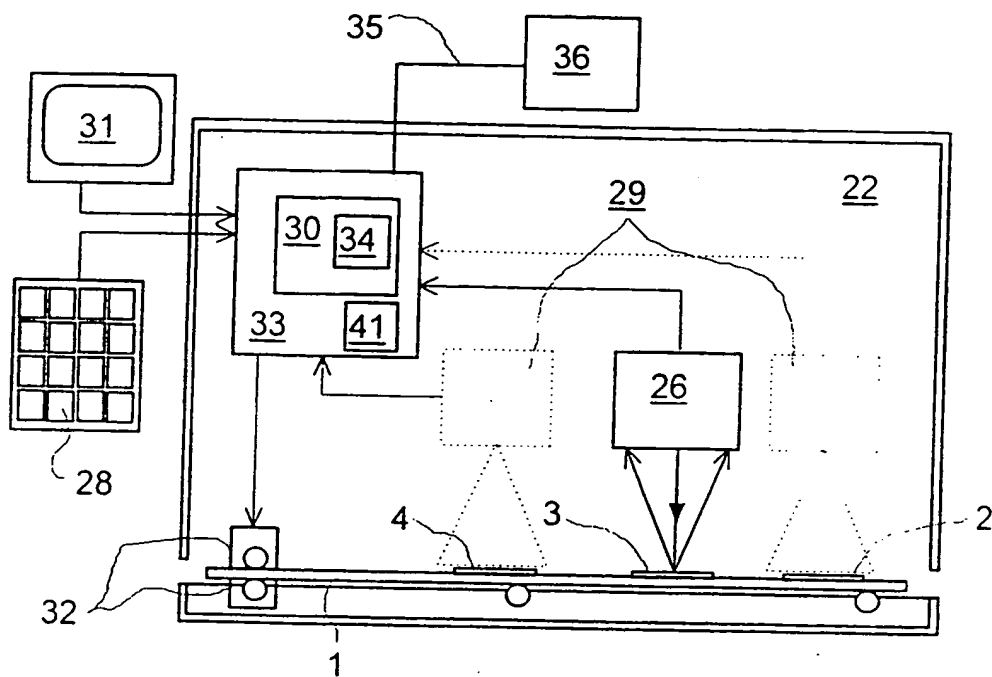


Fig. 7:



INTERNATIONAL SEARCH REPORT

Int. Application No.
PCT/EP 99/10141

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 B42D15/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 B42D

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 3 833 795 A (SHOSHANI ET AL) 3 September 1974 (1974-09-03) cited in the application the whole document	1,8
A	EP 0 718 795 A (LANDIS & GYR TECHNOLOGY INNOVATION) 26 June 1996 (1996-06-26) cited in the application the whole document	1,8

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

12 April 2000

Date of mailing of the international search report

25/04/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-2040

Authorized officer

Franc A

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP 99/10141

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 3833795	A	03-09-1974	IL 37456 A	15-10-1975
			DE 2237911 A	01-03-1973
			FR 2149863 A	30-03-1973
			JP 48026346 A	06-04-1973
			NL 7210717 A	07-02-1973
EP 718795	A	26-06-1996	CN 1157972 A	27-08-1997
			FI 956186 A	23-06-1996
			JP 8263841 A	11-10-1996
			NO 955158 A	24-06-1996

INTERNATIONALER RESEARCHENBERICHT

Int. Aktenzeichen

PCT/EP 99/10141

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES

IPK 7 B42D15/10

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierte Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 7 B42D

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	US 3 833 795 A (SHOSHANI ET AL) 3. September 1974 (1974-09-03) in der Anmeldung erwähnt das ganze Dokument	1,8
A	EP 0 718 795 A (LANDIS & GYR TECHNOLOGY INNOVATION) 26. Juni 1996 (1996-06-26) in der Anmeldung erwähnt das ganze Dokument	1,8

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"A" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

12. April 2000

Abschließdatum des internationalen Recherchenberichts

25/04/2000

Name und Postanschrift der Internationalen Recherchenbehörde

Europäisches Patentamt, P.B. 5818 Patentaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax (+31-70) 340-2040

Bevollmächtigter Bediensteter

Evans A

INTERNATIONALE RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP 99/10141

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 3833795 A	03-09-1974	IL 37456 A	15-10-1975
		DE 2237911 A	01-03-1973
		FR 2149863 A	30-03-1973
		JP 48026346 A	06-04-1973
		NL 7210717 A	07-02-1973
EP 718795 A	26-06-1996	CN 1157972 A	27-08-1997
		FI 956186 A	23-06-1996
		JP 8263841 A	11-10-1996
		NO 955158 A	24-06-1996